GDPR Policy 2023

Contents

Cedar, a recruitment business, is a holder and processor of personal data and generates its revenue through the legitimate introduction of candidates to clients.

A candidate is defined as an individual who has previously indicated that they are interested in engaging with cedar with the purpose of us introducing potential new career opportunities to them. We will have been sent a copy of their CV which will either have been submitted by them in relation to a specific role or submitted so that we might be aware that they are keen on hearing about potential roles

A client is defined as an organisation who may have a suitable career opportunity for one of our candidates. This client may be an active client who is either currently working with us, a historic client who has worked with us in the past or a prospect client who may work with us in the future.

A. Lawful basis for holding and processing data – by either consent or legitimate business interest as defined as "finding work services" for candidates

- Cedar hold / process data in order to provide "finding work" services to our candidates
- We define "finding work services" as the process whereby we introduce potential employment opportunities / potential future employers to candidates. Thereafter we may introduce a candidate's details to potential employers (clients)
- We would only introduce a candidate's details to a client with the explicit prior agreement of the candidate
- We do nothing with candidate data other than providing "finding work services" and providing "career advisory services"
- For a full list of our reasons for holding and processing your data, please click here or see section (o) of this document

B. Lawful basis for holding and processing data – by either consent or legitimate business interest as defined as "career advisory" for candidates

- Cedar holds / processes data in order to provide candidates with valuable market information and career advice. This information may allow candidates to make themselves more marketable to potential clients and understand better how they can work with cedar in order that we can help them secure their next career move.
- We do nothing with candidate data other than providing "finding work services" and providing "career advisory services"
  For a full list of our reasons for holding and processing your data, please click here or see section (o) of this document.

C. Lawful basis in holding and processing data as a legitimate business interest in relation to client and candidate data

- Cedar will hold / process data to facilitate the effective introduction of candidates to clients.
- **Definition - A candidate** is defined as an individual who has previously indicated that they are interested in engaging with cedar with the purpose of us providing them with "find work services". We will have been sent a copy of their CV which will either have been submitted by them in relation to a specific role or submitted so that we might be aware that they are keen on hearing about other potential roles in the future.
- **Definition - A client** is defined as an individual within an organisation who may have a suitable career opportunity for one of our candidates. This client may be an active client who is either currently working with us, a historic client who has worked with us in the past or a prospect client who may work with us in the future.
- The process of introducing a candidate to a client is considered the core nature of cedar's business. By definition, it is a legitimate business interest of cedar's to assist candidates with "finding work services" and this would be impossible without the introduction of their details (with their consent) to clients nor without general communication with clients.
- It is a legitimate business interest for cedar to be in contact with any individual client contact for the purposes of candidate introduction so that they might be aware of potential new employees who they might hire.
- It is a legitimate business interest for cedar to be in contact with any individual client contact for the purposes of sharing valuable market information relating to attracting and retaining candidates, career management / advisory matters and current market news. This contact will allow current and prospect clients to be more likely to use cedar's recruitment services thus allowing us to be more effective in providing "finding work services" to our candidates.
- It is a legitimate business interest for cedar to be in contact with any individual client contact for the purposes of turning the individual client contact into a future candidate who we will then be able to offer "finding work services" to
- It is a legitimate business interest for cedar to be in contact with any individual client contact for the purposes of the sharing of information relating to cedar's recruitment services. This contact will allow current and prospect clients to be more likely to use cedar's recruitment services thus allowing us to be more effective in providing "finding work services" to our candidates
- Consent to send candidate details to any client and all contact with any client will always be recorded on cedar's CRM (Voyager Infinity).
- For a full list of our reasons for holding and processing your data, please click here or see section (o) of this document.

D. Lawful basis in holding and processing data as a legitimate business interest in relation to current and previous employees

- Cedar will hold / process data in relation to current and past employees to ensure compliance with any of our legal obligations
- Cedar will hold / process data in relation to current and past employees to allow us to perform our contract with current employees and in some instances we may use employee personal information for our legitimate business interests or those of third parties provided that the employees interests and fundamental rights do not override those interest
  For a full list of our reasons for holding and processing your data, please click here or see section (o) of this document

E. The right to rectify information, withdraw consent or complain – this information needs to be available easily (on website and in email format should anyone request it)

- **You will at any stage have the right to rectify you information**
- In order to rectify information, please contact us at datacompliance@cedarrecruitment.com which information you need to change. If you do not hear back from us within 48 hours then please contact Kirsty McBean on 0203 002 8050 km@cedarrecruitment.com. If you do not hear back from Kirsty McBean within 48 hours then please contact Jayne Halperin jayneh@cedarrecruitment.com or Howard Bentwood howard@cedarrecruitment.com
- If you do not know the name of your cedar consultant, then in the first instance please contact Kirsty McBean

- You can change your preferences at any stage through the preference centre (found either on our website or on any email communication we send to you). Here is a link to our marketing preferences.

- **You will at any stage have the ability to withdraw consent**
- In order to withdraw consent, please contact Cedar by email datacompliance@cedarrecruitment.com requesting that you no longer wish for us to handle / process your data. If you do not hear back from your cedar consultant with 48 hours then please contact Kirsty McBean on 0203 002 8050 km@cedarrecruitment.com. If you do not hear back from Kirsty McBean within 48 hours then please contact Jayne Halperin jayneh@cedarrecruitment.com or Howard Bentwood howard@cedarrecruitment.com.
- This process is fully outlined in our privacy policy on our website or in this link here or see section (o) of this document

- **You will at any stage have the ability to complain**
- In order to complain, please send an email to Kirsty McBean and cc'ing Jayne Halperin and Howard Bentwood outlining your complaint (email addresses are listed below)
- This email will be responded to within 48 hours
- Kirsty McBean 0203 002 8050 km@cedarrecruitment.com
- Jayne Halperin 0203 002 8050 jayneh@cedarrecruitment.com
- Howard Bentwood 0203 002 8050 howard@cedarrecruitment.com
- Or email - datacompliance@cedarrecruitment.com
- This process is fully outlined in our Privacy Policy on our website or in this link here or see section (o) of this document.

F. Data retention policy

This data retention policy sets out the obligations of **Cedar** ("us/we/our") and the basis upon which we shall retain, review and destroy data held by us, or within our custody or control.

This policy applies to our entire organisation including our officers, employees, agents and sub-contractors and sets out what the retention periods are and when any such data may be deleted.

We are registered under the Information Commissioner's Office under registration number Z1396642.

Objectives

It is necessary to retain and process certain information to enable our business to operate. We may store data in the following places:

- our own servers;
- any third-party servers;
- potential email accounts;
- desktops;
- employee-owned devices (BYOD);
- potential backup storage; and/or
- our paper files.

This policy applies equally to paper, electronic media and any other method used to store personal data. The period of retention only commences when the record is closed.

We are bound by various obligations under the law in relation to this and therefore, to comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation 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 out the procedures that are to be followed when dealing with personal data and how we aim to comply with the Regulation in so far as it is possible. In summary, the Regulation states that all personal data shall be:

(a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;
(b) 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;
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
(d) 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 they are processed, is erased or rectified without delay;
(e) 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 Regulation in order to safeguard the rights and freedoms of the data subject;

(f) 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.

The Fourth and Fifth Data Protection Principles require that any data should not be kept longer than necessary for the purpose for which it is processed and when it is no longer required, it shall be deleted and that the data should be adequate, relevant and limited for the purpose in which it is processed.

With this in mind, this policy should be read in conjunction with our other policies which are relevant such as our data protection policy and IT security policy.

Security and Storage

All data and records are stored securely to avoid misuse or loss. We will process all personal data we hold in accordance with our IT Security Policy **OR** take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data].

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if there is agreement by them to comply with those procedures and policies, or if there are adequate measures in place.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the cedar's central computer system instead of individual PCs.

From time to time, it may be necessary to retain or access historic personal data under certain circumstances such as if we have contractually agreed to do so or if we have become involved in unforeseen events like litigation or business disaster recoveries.

Destruction and Disposal

Upon expiry of our retention periods, we shall delete confidential or sensitive records categorised as requiring high protection and very high protection, and we shall either delete or anonymise less important documents.

Our team including Kirsty McBean, Laura Paterson, Howard Bentwood (or any other members of the back office support team at Cedar) are responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of confidential, financial, and personnel-related records shall be securely destroyed electronically or by shredding if possible. Non-confidential records may be destroyed by recycling.

G. Record table for retaining / holding data and data purging timelines

Cedar is a recruitment business with a legitimate business interest in holding / processing data. Listed below is a schedule of the type of data we hold, the reason we hold it and the length of time we will retain it. Definitions of different categories of individual whose data cedar hold:

- **Placed permanent candidate:** an individual who we have introduced to a client who has been subsequently hired them into a permanent role within their organisation.

- **Placed temporary candidate:** an individual who we have introduced to a client who has subsequently been hired them into non-permanent (temporary) role within their organisation. The temporary candidate may be working for the client organisation through a limited company, an umbrella company or as a PAYE employee through cedar

- **Active candidate:** an individual who has previously indicated that they are interested in engaging with cedar with the purpose of us providing them with "find work services". We will have been sent a copy of their CV which will either have been submitted by them in relation to a specific role or submitted so that we might be aware that they are keen on hearing about other potential roles in the future. An active candidate will be in "active dialogue" with us (by email / telephone / text / LinkedIn / other social media platforms). This active dialogue will occur a minimum of once a year. We need to hold data for active candidates so that we might provide them with "finding work services"

- **Inactive (passive) candidate:** an individual who has previously indicated that they are interested in engaging with cedar with the purpose of us providing them with "find work services". We will have been sent a copy of their CV which will either have been submitted by them in relation to a specific role or submitted so that we might be aware that they are keen on hearing about other potential roles in the future. An inactive (passive) candidate will not have been in contact with us / responded to any contact from us (by email / telephone / text / LinkedIn / other social media platforms) for more than one year but less than 5 years. We need to hold data for inactive (passive) candidates so that we might provide them with "finding work services" even if they are not actively searching for a new role (but who haven't withdrawn consent for us to hold their data)

- **Inactive (historic) candidate:** an individual who has previously indicated that they are interested in engaging with cedar with the purpose of us providing them with "find work services". We will have been sent a copy of their CV which will either have been submitted by them in relation to a specific role or submitted so that we might be aware that they are keen on hearing about other potential roles in the future. An inactive candidate will not have been in contact with us / responded to any contact from us (by email / telephone / text / LinkedIn / other social media platforms) for more than 5 years.

- **Active client:** a client who we are currently working with, have historically worked with or who we may work with

- **Inactive client:** a client who we have historically worked with or who we have tried to work with but who hasn't been in contact with us for more than 10 years

- **Current cedar employee:** an individual who is currently employed by cedar but who is not acting as a temporary candidate for one of cedar's clients

- **Historic cedar employee:** an individual who was historically employed by cedar (but not in the capacity as a temporary candidate for one of cedar's clients)

Type of data	**Data purging timescale**
Placed permanent candidate	15 years from last contact with candidate
Placed temporary candidate	15 years from last contact with candidate
Active candidate	removed after 5 years of no contact with candidate
Inactive (passive) candidate	removed after 5 years of no contact with candidate
Inactive (historic) candidate	removed after 5 years of no contact with candidate
Current cedar employee	not applicable
Historic cedar employee	removed 15 years after employment ceased
Individual Client data	removed after 15 years if no contact from individual client

H. Data purging process

- Every month we will carry out a search of the entire candidate database and remove all those inactive (historic) candidates who have not been in contact with us for more than 5 years
- All purged details will be fully delated from cedar's database and will be non-accessible thereafter

I. Cookies policy, websites terms of use and privacy / transparency policy

- Cookies policy can be found here, website terms of use can be found here and privacy / transparency policy can be found here or see section (o) of this document

J. Preference settings / opt in / opt out / unsubscribe links on emails

- All emails from cedar will have preference settings / opt in / opt out / unsubscribe links. These signatures are centrally managed whereby individual users cannot change, amend or edit prior to sending out. This ensures that any recipient of an email can effectively and easily manage how we cedar are using their data. This might include updating / changing their preferences or complete removal of all data.

K. Data protection policy

1. Our specific data protection measures are as follows:

Encryption	All offsite backups to Netflo are encrypted in transit and at rest
Transmission via email	TLS encryption where possible, depending on third party email system. Outlook and mobile clients have encrypted connections to Office365

Storage of emails and email content	Emails are stored on Office365. Access is granted only via complex passwords.
Access of third parties	Netflo access our systems using TeamViewer which is encrypted and with a complex password. Voyager access line of business systems using Remote Desktop via secure Remote Desktop Gateway.
Storage of electronic copies	Access to electronic information on the servers can only be accessed via passwords
Sharing	Other than emails, there is no form of sharing of information.
Passwords	Passwords on Office365 are complex. However internal machines use a simple password which would need to be made complex, to be compliant.

Our use of personal data and our purpose

Cedar is a recruitment business with a legitimate business interest in holding / processing data. Listed below is a schedule of the type of data we hold, the reason we hold it and the length of time we will retain it. Definitions of different categories of data which cedar may collect, hold and/or process are as follows:

- **Placed permanent candidate:** an individual who we have introduced to a client who has been subsequently hired them into a permanent role within their organisation.

- **Placed temporary candidate:** an individual who we have introduced to a client who has subsequently been hired them into non-permanent (temporary) role within their organisation. The temporary candidate may be working for the client organisation through a limited company, an umbrella company or as a PAYE employee through cedar

- **Active candidate:** an individual who has previously indicated that they are interested in engaging with cedar with the purpose of us providing them with "find work services". We will have been sent a copy of their CV which will either have been submitted by them in relation to a specific role or submitted so that we might be aware that they are keen on hearing about other potential roles in the future. An active candidate will be in "active dialogue" with us (by email / telephone / text / LinkedIn / other social media platforms). This active dialogue will occur a minimum of once a year. We need to hold data for active candidates so that we might provide them with "finding work services"

- **Inactive (passive) candidate:** an individual who has previously indicated that they are interested in engaging with cedar with the purpose of us providing them with "find work services". We will have been sent a copy of their CV which will either have been submitted by them in relation to a specific role or submitted so that we might be aware that they are keen on hearing about other potential roles in the future. An inactive (passive) candidate will not have been in contact with us / responded to any contact from us (by email / telephone / text / LinkedIn / other social media platforms) for more than one year but less than 5 years. We need to hold data for inactive (passive) candidates so that we might provide them with "finding work services" even if they are not actively searching for a new role (but who haven't withdrawn consent for us to hold their data)

- **Inactive (historic) candidate:** an individual who has previously indicated that they are interested in engaging with cedar with the purpose of us providing them with "find work services". We will have been sent a copy of their CV which will either have been submitted by them in relation to a specific role or submitted so that we might be aware that they are keen on hearing about other potential roles in the future. An inactive candidate will not have been in contact with us / responded to any contact from us (by email / telephone / text / LinkedIn / other social media platforms) for more than 5 years.

- **Current cedar employee:** an individual who is currently employed by cedar but who is not acting as a temporary candidate for one of cedar's clients.

- **Historic cedar employee:** an individual who was historically employed by cedar (but not in the capacity as a temporary candidate for one of cedar's clients).

<u>Section A: Overview</u>

2. The reason for this policy

2.1 You have legal rights with regard to the way your personal data is handled.

2.2 In the course of our business activities we collect, store and process personal data about our customers, suppliers and other third parties and therefore, in order to comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this data.
All people working in or with our business are obliged to comply with this policy when processing personal data.

3. Introduction

3.1 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, for example, customers and business contacts, or that is provided to us by data

subjects or other sources.

3.2 In this policy when we say "you' or "your" we are generally referring to the data subjects unless the context requires otherwise.

3.3 It also sets out our obligations in relation to data protection under the General Data Protection Regulation 2016 ("the **GDPR Rules**").

3.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

3.5 We agree to ensure that all of our directors, employees, consultants and agents comply with this policy.

3.6 We aim to ensure the correct, lawful, and fair handling of your personal data and to respect your legal rights.

4. The meaning of key Data Protection terms

4.1 **data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

4.2 **data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

4.3 **personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

4.4 **data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

4.5 **processing** is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

5. Summary of the Data Protection Principles

This Policy aims to ensure compliance with the GDPR Rules. The GDPR Rules sets out the following principles with which any party handling personal data must comply. All personal data must be:

(a) **Processed fairly and lawfully** – it must be processed fairly and lawfully and it must be processed - in relation to you as the data subject - in a transparent manner

(b) **Processed for limited purposes and in an appropriate way -** the purposes for which it is collected must be explicit, specified and legitimate

(c) **Adequate, relevant and not excessive for the purpose**

(d) **Accurate** – as well as being accurate it must be kept up to date with inaccurate data deleted

(e) **Not kept longer than necessary for the purpose**

(f) **Processed in line with data subject's rights**

(g) **Security** – there must appropriate technical or organisational measures to ensure appropriate security

In addition, personal data must not be transferred outside the European Economic Area (the "**EEA**") without **adequate protection.**

<u>Section B: Data Protection Principles</u>

6. Notifying Data Subjects

As part of complying with the principles in para 4 above, if you provide us with personal data we will always try to tell you:

6.1 the purpose or purposes for which we intend to process that personal data

6.2 the types of third parties, if any, with which we will share or to which we will disclose that personal data

6.3 how you can limit our use and disclosure of their personal data

6.4 if we receive personal data from other sources.

7. Lawful, Fair, and Transparent Data Processing

The GDPR Rules are not intended to prevent the processing of personal data but to ensure that it is done fairly and without adversely affecting your rights. The processing of personal data is lawful if one (or more) of the following applies:

(a) **(consent)** the data subject has consented for a specific purpose;

(b) **(contract**) if the data subject requests the processing with a view to entering into a contract or the processing is necessary for the performance of a contract

(c) **(legal obligation)** if the processing is necessary for the compliance with a legal obligation to which the data controller is subject

(d) **(protection)** processing is necessary to protect your vital interests or those of another natural person

(e) **(public interest)** it is in the public interest for a task to be carried out which requires such processing, or the task is to be carried out as a result of the exercise of any official authority held by the data controller;

(f) **(legitimate interests)** for the legitimate interest of the data controller or the party to whom the personal data is disclosed.

8. Processed for limited purposes and in an appropriate way

8.1 In the course of our business, we may collect and process the personal data set out above. This may include personal data we receive directly from you (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

8.2 We will only process personal data for the specific purposes set out above or for any other purposes specifically permitted by the GDPR Rules. We will notify those purposes to you when we first collect the personal data or as soon as possible thereafter.

9. Adequate, Relevant and not excessive for the purpose

We will only collect and process personal data for the specific purpose(s) set out above.

10. Accuracy of Data and Keeping Data Up To Date

We will keep your personal data accurate and up-to-date. We will check its accuracy regularly. When we find inaccurate or out-of-date data we will take reasonable steps to amend or erase that data.

11. Timely Processing

We will only keep your personal data for a period of time which we judge is relevant and necessary taking into account the purpose(s) of collecting the personal data which are specified above.

12. Processing that is secure

In addition to the measures above:

12.1 we will make sure that the personal data we collect is securely kept and we stop unauthorised processing and prevent its loss, destruction or damage

12.2 we will ensure that only people who are authorised to use personal data can access it and that we have entry controls to our premises and systems, lockable desks and cupboards for confidential personal data and destruction of hard copy documents and digital storage devices

12.3 all authorised persons must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

<u>Section C: Data Subject Rights</u>

13. You, as a data subject, have the right to information about:

(a) who we are

(b) the purpose(s) of collecting your personal data and the legal basis for collecting it and what our legitimate interest is for processing your personal data

(c) the categories of personal data collected and where is to be transferred, especially if outside the EEA

(d) the length of time we hold personal data (or, where there is no predetermined period, details of how that length of time will be determined)

(e) your rights as a data subject including your right to withdraw your consent to processing, the right to complain to the Information Commissioner and also things such as details of any legal requirement for processing personal data that may exist and any automated decision-making that we carry out.

We will try to provide this information when we collect the personal data or, if we collect the personal data from another party, when we communicate with you after the personal data is received.

14. Data Subject Access

14.1 You may request access to any data held about you by us (a subject access request ("**SAR**")

14.2 We reserve the right to charge reasonable fees for onerous or repetitive requests.

14.3 Data subjects must make a formal request for information we hold about them. This must be made in writing.

14.4 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) we will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) we will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

15. Accuracy of personal data: right to rectification

15.1 We will do our best to ensure that all personal data held about you is accurate and complete. We ask that you notify us of any changes to information held about you.

15.2 You have the right to request that any incomplete or inaccurate information held about you is rectified and to lodge a complaint with us and the Information Commissioner's Office.

15.3 We will respond to requests to rectify within one month.

16. Right to be forgotten

You have the right to request the deletion or removal of personal data however requests for erasure can be rejected in certain circumstances.

17. Right to restriction of Processing

You can block the processing of your personal data. This means we may be able to store it, but cannot process it further without consent. Restricting data is required where the accuracy of data is challenged - but only until the accuracy has been verified.

18. Right to data portability

18.1 If you have provided personal data to us you have the right to transfer it from us to someone else.

18.2 If you request it, we may be required to transmit the data directly to another organisation if feasible. We must respond without undue delay and within one month, or two months if the request is complex.

19. The right to object

You have a right to object to the processing of your data. We must stop processing unless we can demonstrate a legal ground for the processing.

20. Automated decision-making

20.1 You have the right not to be subject to a decision based on automated processing and it produces a legal effect or other significant effect on you.

20.2 You can request human intervention where personal data is processed using automated decision-making and can ask for an explanation of the decision to use automated decision-making.

Section D: Our Other Obligations

21. How we deal with personal data internally

21.1 We will:

(a) train our employees in relation to our responsibilities under the GDPR Rules

(b) ensure that only appropriately trained, supervised and authorised personal have access to personal data held by us; and

(c) regularly evaluate and review our collection and processing of personal data and the performance of employees and third parties working on our behalf to ensure that it is in accordance with the GDPR Rules.

21.2 We will keep internal records of personal data that we collect and process including, in relation to that personal data, details of the categories, any transfers, our security measures, our purpose of collection and the duration of retention of that personal data. We will also retain details of all third parties that either collect your personal data for us or that we use to process your personal data.

21.3 We will carry out privacy impact assessments as required by law.

22. Transferring personal data to a country outside the EEA

We may transfer personal data to countries outside of the EEA however we will ensure that the transfer is:

(a) to a place that the EU has judged to provide adequate levels of protection for personal data

(b) to a place that provides adequate safeguards under either an agreement with a public body, rules that bind companies or standard data protection clauses adopted by the EU or some other form of approved code of conduct approved by a supervisory authority or certification or other contractual clauses or regulatory provisions

(c) necessary for the performance of a contract between you and us or with a view to creating that contract

(d) made with your consent

(e) necessary for important public interest reasons, legal claims, to protect your vital interests

23. Notification of personal data security breach

23.1 If a personal data security breach occurs, we will manage and respond to it effectively in accordance with GDPR and it must be reported immediately to our Data Protection Officer.

23.2 We will notify the Information Commissioners Office (**ICO**) and any data subject of personal data security breaches to the extent we are required to do so by GDPR.

23.3 If disclosure is not required by GDPR, we will nevertheless investigate closely all the circumstances surrounding the breach and examine the seriousness of the breach and the benefits that might be obtained by disclosure (such as limiting risks of fraud) and we will give careful consideration to any decision to notify the ICO or you, especially if your rights and freedoms as data subjects are affected.

L. Data security Policy

1. Introduction

The security and integrity of their IT Systems is a priority for **Cedar** (the "Company"). All employees of the Company and any authorised third parties, including without limitation, sub-contractors, consultants and contractors (together "Users") are expected to comply with this Policy, which is effective from the date above, but subject to being updated from time to time.

2. Intended purpose

The purpose of this Policy is to establish a framework for managing risks and protecting the Company's IT infrastructure, computing environment, hardware, software and any and all other relevant equipment ("IT Systems") against all types of threats, internal or external, intentional or unintentional.

3. Stakeholder Responsibilities

3.1 **Netflo** (the "IT Department") shall be responsible for carrying out the installation, ongoing maintenance (including without limitation, any upgrades or repairs) and ensuring the security and integrity of the IT Systems, either directly or, via an authorised third party. Accordingly, the IT Department is responsible for data stored on the IT system unless otherwise stated.

3.2 In furtherance of section 3.1 above, the IT Department shall be responsible for:

(a) investigating any security breaches and / or misconduct, and shall escalate to Kirsty McBean or Howard Bentwood as appropriate;
(b) regularly reviewing IT security standards within the Company and ensuring the effective implementation of such standards, by way of periodic audits and risk assessments, with regular reports being made to the Company's internal senior management shall be responsible on the condition of the Company's information security and compliance with this Policy;
(c) ensuring organisational management and dedicated staff responsible for the development, implementation and maintenance of this Policy;
(d) providing assistance as necessary to Users to help them in their understanding and compliance with this Policy, as well as keeping all Users aware and up to date with all applicable laws including, without limitation, the GDPR and the Computer Misuse Act 1990.
(e) providing adequate training and support in relation to IT security matters and use of the IT Systems, to all Users
(f) ensuring that the access to IT Systems granted to all Users takes into account their job role, responsibilities and any additional security requirements, so that only necessary access is granted for each User
(g) dealing with all reports, whether from Users or otherwise, relating to IT security matters and carrying out a suitable response for the situation
(h) implementing appropriate password controls, as further detailed in section 5.
(i) maintaining a complete list of all hardware items within the IT Systems. All such hardware shall be labelled and the corresponding data shall be kept by the IT Department;
(j) ensuring that **daily** backups of all data stored within the IT Systems are taken, and that all such backups are stored off the Company premises at a suitably secure location; and
(k) [ensure compliance with all IT security standards set out in ISO 27001, to the extent such standards are not covered by the obligations set out in section 3.2 (a) – (j)].

3.3 The Users shall be responsible for:

(a) informing the IT Department immediately of any actual or potential security breaches or concerns relating to the IT Systems;
(b) informing the IT Department immediately in respect of any technical or functional errors experienced relating to the IT Systems; and
(c) complying with this Policy and all laws applicable to the Users relating to their use of the IT Systems.

3.4 Users must not attempt to resolve an IT security breach on their own without consulting the IT Department first.

4. Access to IT Systems

4.1 There shall be logical access controls designed to manage electronic access to data and IT System functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all Users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

4.2 All IT Systems shall only be accessible by a secure log-in system as deemed suitable by the IT Department. Such suitable systems may include, without limitation, secure passwords, fingerprint identification and facial recognition.

4.3 The IT Department shall conduct regular system audits or event logging and related monitoring procedures to proactively record User access and activity on the IT Systems for routine review.

4.4 IT Systems that are not intended to be part of everyday use by most Users (including without limitation, servers, networking equipment and infrastructure) and any other areas where personal data may be stored (eg. data centre or server room facilities) shall be designed to:

(a) protect information and physical assets from unauthorised physical access;
(b) manage, monitor and log movement of persons into and out of the relevant facilities; and

(c) guard against environmental hazards such as heat, fire and water damage.

5. Passwords

5.1 The IT Department shall implement password controls designed to manage and control password strength, expiration and usage including prohibiting Users from sharing passwords and requiring that the Company passwords that are assigned to Users:

(a) be at least 3 characters in length,
(b) not be stored in readable format on the Company's IT Systems;
(c) must be changed every 365 days;
(d) must have defined complexity;
(e) must have a history threshold to prevent reuse of recent passwords; and
(f) newly issued passwords must be changed after first use.

5.2 Users must keep passwords confidential and not share it with anyone else.

6. Hardware

6.1 All Company mobile devices (including, without limitation, laptops, tablets and mobile telephones) should be kept securely by Users using secure cases where appropriate. Users should not leave such mobile devices unattended other than at their homes or Company premises.

6.2 All Company non-mobile devices (including, without limitation, desktop computers, workstations and monitors) shall, wherever possible and practical, be secured in place with a suitable locking mechanism.

6.3 Users are not permitted to connect any of their personal hardware to the IT Systems without the express approval of the IT Department in writing.

7. Software

7.1 All software installation on to the IT Systems shall be the responsibility of the IT Department. Users are not permitted to install any software on to the IT Systems unless expressly approved in writing by the IT Department.

7.2 All software installed on to the IT Systems shall be kept sufficiently up to date in order to ensure that the security and integrity of the IT Systems is not compromised.

8. Vulnerability Assessment and Anti-Virus

8.1 The IT Department shall carry out regular vulnerability assessments, and utilise patch management, threat protection technologies and scheduled monitoring to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

8.2 The IT Department shall ensure that the Company uses an up to date reputable anti-virus checking software tool to check the IT Systems and to scan all email attachments before they are opened.

Users may download files from any cloud storage systems, subject to prior approval from the IT Department; and Users shall permit any such files to be scanned for viruses as part of the download process.

8.3 The IT Department shall implement network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

9. Data Protection

9.1 The collection, holding and processing of all personal data (as defined in the General Data Protection Regulation 2016 ("GDPR")) by the Company will be carried out in compliance with (i) the GDPR and (ii) the Company's own Data Protection Policy.

9.2 The IT Department shall ensure there are data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for personal data that is:

(a) transmitted over public networks (i.e. the Internet) or when transmitted wirelessly;

or

(b) at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).

9.3 All emails containing personal data must be encrypted.

9.4 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 therewith should also be deleted.

9.5 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.

9.6 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.

9.7 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 the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

9.8 The IT Department shall ensure operational procedures and controls to provide to provide for the secure disposal of any part of the IT Systems or any media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Company's possession.

9.9 Where 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. Hardcopies should be shredded, and electronic copies should be deleted securely.

9.10 The IT Department shall ensure that it has in place appropriate technical and organisational measures, to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it).

9.11 All personal data stored electronically should be backed up daily with backups stored onsite AND/OR offsite. All backups should be encrypted.

9.12 All electronic copies of personal data should be stored securely using passwords and data encryption.

9.13 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Kirsty McBean and/or Laura Paterson position(s) km@cedarrecruitment.com or lp@cedarrecruitment.com to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least annually.

9.14 Only Users 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.

9.15 All Users that have access to, and handle personal data on the Company's behalf, shall adhere to the Company's Data Protection Policy.

10. Business Continuity

The Company shall have in place adequate business resiliency/continuity and disaster recovery procedures designed to maintain any information and the supply of any service and/or recovery from foreseeable emergency situations or disasters.

11. Email and Internet

Please refer to the Company's policy on Email and Internet usage in respect of email and internet use on the IT Systems

12. Training

Security awareness training for Users shall be provided by the IT Department. Training will be provided at different levels for different Users based on their role. Users may request retraining after 2 years.

Breaches of this policy

If you consider that this policy has not been followed in respect of personal data about yourself or others you should raise the matter with your Kirsty McBean, Jayne Halperin or Howard Bentwood.

- Kirsty McBean 0203 002 8050 at km@cedarrecruitment.com
- Jayne Halperin 0203 002 8050 jayneh@cedarrecruitment.com
- Howard Bentwood 0203 002 8050 howard@cedarrecruitment.com
- Or by emailing – datacompliance@cedarrecruitment.com

M. Staff training

- All staff will be trained on using cedar's CRM (Voyager Infinity) so that any candidates details are help and processed in compliance with GDPR.
- All staff will be trained on using cedar's CRM (Voyager Infinity) so that any client contact is made in a manner compliant with GDPR.
- All staff will be trained as to what action to take in the event that any client or candidate wishes to amend or rectify their information, withdraw consent or complain.
- in relation to the last point, all staff are aware of the following key internal contacts and that they need to inform the key contacts within 48 hours of any request
    - Kirsty McBean 0203 002 8050 at km@cedarrecruitment.com
    - Jayne Halperin 0203 002 8050 jayneh@cedarrecruitment.com
    - Howard Bentwood 0203 002 8050 howard@cedarrecruitment.com

N. Privacy notice to staff

What is the purpose of this document?

You have legal rights about the way your personal data is handled by us, **cedar recruitment ltd**. We are committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us. It applies to all employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

During your employment or engagement by us, we collect, store and process personal data about you. To comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this data.

It is important that you read this notice, along with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you. This gives you information about how and why we are using such information. All people working in or with our business are obliged to comply with this policy when processing personal data.

Our Role

We are a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. Data protection legislation requires to give you the information contained in this privacy notice.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have explained to you clearly and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited to those purposes only.
- Accurate and kept up to date.
- Kept only for such time as is necessary for the purposes we have told you about.
- Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are "special categories" of more sensitive personal data that require a higher level of protection.

We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information, bonus and commissions details.
- Start date.
- Location of employment or workplace.
- Recruitment information (including copies of passport or other right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).

- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- Information about your use of our information and communications systems.
- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How is your personal information collected?

Usually we collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information during work-related activities throughout the period of you working for us.

How we will use information about you

We will use your personal information only when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract that applies to our working relationship.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above (see *The kind of information we hold about you*) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases, we may use your personal information for our legitimate interests or those of third parties, provided that your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee or we are under a legal obligation, deducting tax and National Insurance contributions.
- Providing the following benefits to you: Private healthcare
- Liaising with your pension provider.
- Administering the contract that applies to our working relationship with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds that justify our use of your personal information.

If you fail to provide personal information

If you do not provide certain information when we ask for it, we may not be able to perform the contract that applies to our working relationship with you (such as paying you or providing a benefit), or we may not be able to comply with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes that we have collected it for, unless we need to use it for another reason and that reason is reasonable and compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis that allows us to do so.

We may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or allowed by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the situations below:

- In limited circumstances, with your clear written consent.
- Where we need to carry out our legal obligations and in line with our data protection policy or other policy that applies to such information.
- Where it is needed in the public interest, such as for equal opportunities monitoring and in line with our data protection policy or other policy that applies to such information.
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Very occasionally, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family-related leave and related pay, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will give you full details of the information that we would like and the reason we need it, so that you can consider carefully whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy or other policy that applies to such information.

Very occasionally, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We do not envisage that we will hold information about criminal convictions.

Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you while you are working for us.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We can use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision based on any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We may share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: [payroll, pension administration, benefits provision and administration, IT services and healthcare administration.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Transferring information outside the EU]

to ensure that your personal information does receive an adequate level of protection we have put in place appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection:

Data security

We have put in place measures to protect the security of your information. Details of these measures are available here and measures taken in the event of a data breech can be found here.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from CEO/ Internal Ops Manager.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your

personal information are available in our retention policy which is available from the CEO or Internal Operations Manager or here. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy or applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in relation to personal information
Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request that your personal information is erased. This allows you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to stop processing personal information where we are relying on a legitimate interest and there is something about your situation that makes you want to object to processing on this ground.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the CEO or Internal Operations Manager in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the CEO or Internal Operations Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

O. Privacy Policy (candidates / clients / suppliers / users of website)

PRIVACY POLICY

If you're looking for information about how to have your details removed, updated or disclosed to you from Cedar Recruitment Ltd, information on your rights and how to act up on them or if you have any questions relating to data protection please contact us on 0203 002 8050 or datacompliance@cedarrecruitment.com. If you have come to this page because you want to access/ set up your marketing preferences please click here.

INTRODUCTION

For the purpose of applicable data protection legislation (including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR") the company responsible for your personal data ("Cedar" or "us") can be found at:

Cedar Recruitment Ltd, Floor 2 Goldsmiths House, 137 Regent Street, London W1B 4HZ or contacted on 0203 002 8050.

Cedar Recruitment Ltd is registered under the Information Commissioner's Office. Registration Number: **Z1396642.**

Whether we are in the process of helping you find a job, continuing our relationship with you once we have found you a role, providing you with a service, receiving a service from you, using your data to ask for your assistance in relation to one of our candidates and other people whom we may contact in order to find out more about our candidates or whom they indicate is an emergency contact (it also applies to the emergency contacts of our employees) Cedar Recruitment Ltd is committed to protecting the privacy of our users want to provide a safe and secure user experience. We will ensure that the information you submit to us via our website or through our office is only used for the purposes set out in this policy.

This Privacy Policy (together with our Terms of Use and any other documents referred to in it) sets out the basis on which all personal data that we collect from you, or that you provide to us directly and via the cedarrecruitment.com will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we treat it. It describes how we collect, use and process your personal data, and how, in doing so, we comply with our legal obligations to you. Your privacy is extremely important to us and we are committed to protecting and safeguarding your data privacy rights.

Cedar Recruitment Ltd is registered in the UK and this Privacy Policy applies in the UK and EU countries. Different countries may approach data privacy in slightly different ways and we have clearly detailed how we safeguard your data if we need to transfer it internationally where applicable.

If you are dissatisfied with any aspect of our Privacy Policy, you may have legal rights and, where relevant, we have outlined these.

WHAT IF I DO NOT AGREE WITH THIS PRIVACY POLICY?

If you do not agree to our processing of your data in the manner outlined in the Policy, **please do not submit any personal data to us**.

OUR LEGAL BASES FOR PROCESSING YOUR DATA

LEGITIMATE INTERESTS

- Article 6(1)(f) of the GDPR is Cedar's legal basis for processing your data – it stipulates that we can process your data where it "is necessary for the purposes of the legitimate interests pursued by [us] or by a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of [you] which require protection of personal data."

- Cedar does not think that any of the following activities prejudice individuals in any way – in fact; they help us to offer you a more personalised and efficient service. However, you do have the right to object to us processing your personal data on this basis.

- If you would like to know more about how to do so, please refer to section three.

SECTION 1: WHAT INFORMATION WILL WE COLLECT? HOW WILL WE USE IT?

OVERVIEW

We will collect data about you, both personal data (such as your name and contact details) and also sensitive personal data (such as information in your CV). The personal data and sensitive personal data will be stored, processed, used and disclosed by us in the following ways:

- To provide our recruitment services to you and to facilitate the recruitment process
- To assess data about you against vacancies which we judge may be suitable for you
- To send your information to clients in order to apply for jobs or to assess your eligibility for jobs
- To enable you to submit your CV, apply online for jobs or to subscribe to alerts about jobs we think may be of interest to you
- To allow you to participate in interactive features of our service when you choose to do so
- To market our, full range of recruitment services to you (permanent, temporary, contract and recruitment process outsourcing services)
- To enable us to develop and market other products and services and where you have consented to being contacted for such purposes
- To improve our customer service and to make our services more valuable to you (including tailoring our website and our group companies websites when you log on to enrich your personal experience)
- To send you details of reports, promotions, offers, networking and client events and general information about the industry sectors which we think might be of interest to you where you have consented to being contacted for such purposes
- To answer your questions and enquiries
- To third parties where we have retained them to provide services that we, you or our client have requested including references, qualifications and criminal reference checking services, verification of the details you have provided from third party source, psychometric evaluation or skill test
- To third parties, regulatory or law enforcement agencies if we believe in good faith that we are required by law to disclose it in connection with the detection of crime, the collection of taxes or duties, in order to comply with any applicable law or order of a court of competent jurisdiction, or in connection with legal proceedings
- To use your information on an anonymised basis to monitor compliance with our equal opportunities policy
- To carry out our obligations arising from any contracts entered into between you and us

From time to time we may seek your consent to process, use or disclose your information for any other purpose not listed above.

We reserve the right to transfer your information to a third party in the event of a sale, merger, liquidation, receivership or transfer of all or substantially all of the assets of our company provided that the third party agrees to adhere to the terms of this Privacy Policy and provided that the third party only uses your Personal Data for the purposes that you provided it to us. You will be notified in the event of any such transfer and you will be afforded an opportunity to opt-out.

HOW DO WE COLLECT YOUR PERSONAL DATA?

- **CANDIDATE DATA:** We collect candidate personal data in three primary ways:

  1. Personal data that you, the Candidate, give to us;
  2. Personal data that we receive from other sources; and
  3. Personal data that we collect automatically.

Personal data you give to us

Cedar needs to know certain information about you in order to provide a tailored service. This will enable us to provide you with the best opportunities, and should save you time in not having to trawl through information about jobs and services that are not relevant to you.

There are numerous ways you can share your information with us. It all depends on what best suits you or the basis in which you are contacting us. These may include:

- Entering your details on the Cedar website or via an application form, as part of the registration process;
- Leaving a hard copy CV at a Cedar recruitment event or office;
- Emailing your CV to a Cedar consultant or being interviewed by them;
- Applying for jobs through a job aggregator, which then redirects you to the Cedar website;
- Entering a competition through the website, by email or social media channel such as LinkedIn or Twitter.

Personal data we receive from other sources

We also receive personal data about candidates from other sources. Depending on the relevant circumstances and applicable local laws and requirements, these may include personal data received in the following situations:

- Your referees may disclose personal information about you;
- Our clients may share personal information about you with us;
- We may obtain information about you from searching for potential candidates from third party sources, such as LinkedIn and other job sites;
- If you 'like' our social media pages or 'follow' us on Twitter, LinkedIn, Instagram etc. we will receive your personal information from those sites; and
- If you were referred to us through an RPO or an MSP supplier, they may share personal information about you with us.

Personal data we collect automatically.

To the extent that you access our website or read or click on an email from us, where appropriate and in accordance with any local laws and requirements, we may also collect your data automatically or through you providing it to us.

We collect your data automatically via cookies, in line with cookie settings in your browser. If you would like to find out more about cookies, including how we use them and what choices are available to you, please click here.

- **CLIENT DATA:** We collect client personal data in three ways:
    1. Personal data that we receive directly from you;
    2. Personal data that we receive from other sources; and
    3. Personal data that we collect automatically.

Personal data that we receive directly from you

We both share a common goal – to make sure that you have the best talent in your organisation. We will receive data directly from you in two ways:

- Where you contact us proactively, usually by phone or email; and/or
- Where we contact you, either by phone or email, or through our consultants' business development activities more generally.

Personal data we receive from other sources

Where appropriate and in accordance with any local laws and requirements, we may seek more information about you or your colleagues from other sources generally by way of due diligence or other market intelligence including:

- From delegate lists at relevant events;
- From other limited sources and third parties (for example from our candidates to the extent that they provide us with your details to act as a referee for them)
- From third party market research; and
- By analysing online and offline media (which we may do ourselves, or employ other organisations to do for us).

Personal data we collect via our website

To the extent that you access our website or read or click on an email from us, where appropriate and in accordance with any local laws and requirements, we may also collect your data automatically or through you providing it to us.

We collect your data automatically via cookies, in line with cookie settings in your browser. If you would like to find out more about cookies, including how we use them and what choices are available to you, please click here.

- **SUPPLIER DATA:** We need a small amount of information from our suppliers to ensure that things run smoothly.

  We need contact details of relevant individuals at your organisation so that we can communicate with you. We also need other information such as your bank details so that we can pay for the services you provide (if this is part of the contractual arrangements between us).

  To the extent that you access our website or read or click on an email from us, where appropriate and in accordance with any local laws and requirements, we may also collect your data automatically or through you providing it to us.

  We collect your data automatically via cookies, in line with cookie settings in your browser. If you would like to find out more about cookies, including how we use them and what choices are available to you, please click here.

- **PEOPLE WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, SUCH AS REFEREES AND EMERGENCY CONTACTS:** We collect your contact details only where a candidate or a member of our employees puts you down as their emergency contact or where a candidate gives them to us in order for you to serve as a referee.

  In order to provide candidates with suitable employment opportunities safely and securely and to provide for every eventuality for them and our employees, we need some basic background information. We only ask for very basic contact details, so that we can get in touch with you either for a reference or because you've been listed as an emergency contact for one of our candidates or employees members.

- **WEBSITE USERS:** We collect a limited amount of data from our website users which we use to help us to improve your experience when using our website and to help us manage the services we provide. This includes information such as how you use our website, the frequency with which you access our website, and the times that our website is most popular.

A number of elements of the personal data we collect from you are required to enable us to fulfil our contractual duties to you or to others. Where appropriate, some, for example candidates' social security number and, religious affiliation, are required by statute or other laws. Other items may simply be needed to ensure that our relationship can run smoothly. Depending on the type of personal data in question and the grounds on which we may be processing it, should you decline to provide us with such data, we may not be able to fulfil our contractual requirements or, in extreme cases, may not be able to continue with our relationship.

WHAT KIND OF PERSONAL DATA DO WE COLLECT?

- **CANDIDATE DATA:**

  Depending on the relevant circumstances and applicable local laws and requirements, we may collect some or all of the information listed below to enable us to offer you employment opportunities which are tailored to your circumstances and your interests. In some jurisdictions, we are restricted from processing some of the data outlined below. In such cases, we will not process the data in those jurisdictions:

  - Name;
  - Age/date of birth;
  - Birth number;
  - Sex/gender;
  - Photograph;
  - Marital status;
  - Contact details;
  - Education details;
  - Employment history;
  - Emergency contacts and details of any dependants;
  - Referee details;
  - Immigration status (whether you need a work permit);
  - Nationality/citizenship/place of birth;
  - A copy of your driving licence and/or passport/identity card;
  - Financial information (where we need to carry out financial background checks);
  - National Insurance Number (or equivalent in your country) and any other tax-related information;
  - Diversity information including racial or ethnic origin, religious or other similar beliefs, and physical or mental health, including disability-related information;
  - Details of any criminal convictions if this is required for a role that you are interested in applying for;
  - Details about your current remuneration, pensions and benefits arrangements;
  - Information on your interests and needs regarding future employment, collected directly and inferred, for example from jobs viewed or articles read on our website;
  - Extra information that you choose to tell us;
  - Extra information that your referees chooses to tell us about you;
  - Extra information that our clients may tell us about you, or that we find from other third party sources such as job sites;
  - IP address;

  CURRICULUM VITAE ("CV"): We give you the option of submitting your CV via our website or by providing your CV to one of our consultants. You can do this either to apply for a specific advertised job or for consideration by our consultants for positions as they arise. Your CV will be stored in the Cedar Recruitment database, and will be accessible by Cedar's employees in the UK. You can update your CV at any time, simply by following the same procedure to submit a new CV. Your old CV will automatically be archived providing the submission details remain the same (for example you submit both CVs using the same email address or you advise the relevant contact of your new submission).

  N.B. The above list of categories of personal data we may collect is not exhaustive.

- **SUPPLIER DATA:** We don't collect much data about suppliers – we simply need to make sure that our relationship runs smoothly. We'll collect the details for our contacts within your organisation, such as names, telephone numbers and email addresses. We'll also collect bank details, so that we can pay you. We may also hold extra information that someone in your organisation has chosen to tell us. In certain circumstances, such as when you engage with our Finance / Credit Control departments, our calls with you may be recorded, depending on the applicable local laws and requirements.

- **PEOPLE WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, SUCH AS REFEREES AND EMERGENCY CONTACTS:** All we need from referees is confirmation of what you already know about our candidate or prospective employee, so that they can secure a role. Emergency contact details give us somebody to call on in an emergency. To ask for a reference, we will need the referee's contact details (such as name, email address and telephone number). We will also need these details if our candidate or an employee has put you down as their emergency contact so that we can contact you in the event of an accident or an emergency.

- **WEBSITE USERS:** We collect a limited amount of data from our website users which we use to help us to improve your experience when using our website and to help us manage the services we provide. This includes information such as how you use our website, the frequency with which you access our website, your browser type, the location you view our website from, the language you choose to view it in and the times that our website is most popular. If you contact us via

the website, for example by using the chat function, we will collect any information that you provide to us, for example your name and contact details.

SECTION 2: HOW DO WE USE YOUR PERSONAL DATA?

Having obtained data about you, we then use it in a number of ways.

- **CANDIDATE DATA:** The main reason for using your personal details is to help you find employment or other work roles that might be suitable for you. The more information we have about you, your skillset and your ambitions, the more bespoke we can make our service. Where appropriate and in accordance with local laws and requirements, we may also use your personal data for things like marketing, profiling and diversity monitoring. Where appropriate, we will seek your consent to undertake some of these activities.

We generally use Candidate data in four ways:

- Recruitment Activities;
- Marketing Activities;
- Equal Opportunities Monitoring; and
- To help us to establish, exercise or defend legal claims.
- In appropriate circumstances in the future, we may also use Candidate data for Profiling.
- Here are some more details about each:

Recruitment Activities

Our main area of work is recruitment – connecting the right candidates with the right jobs. We have listed below various ways in which we may use and process your personal data for this purpose, where appropriate and in accordance with any local laws and requirements. Please note that this list is not exhaustive.

- Collecting your data from you and other sources, such as LinkedIn;
- Storing your details (and updating them when necessary) on our database, so that we can contact you in relation to recruitment;
- Providing you with our recruitment services and to facilitate the recruitment process;
- Assessing data about you against vacancies which we think may be suitable for you;
- Sending your information to Clients, in order to apply for jobs or to assess your eligibility for jobs;
- Enabling you to submit your CV, apply online for jobs or to subscribe to alerts about jobs we think may be of interest to you;
- Allowing you to participate in specialist online training;
- Allowing you to participate in the interactive features of our services, when you choose to do so;
- Carrying out our obligations arising from any contracts entered into between us;
- Carrying out our obligations arising from any contracts entered into between Cedar and third parties in relation to your recruitment;
- Facilitating our payroll and invoicing processes;
- Carrying out customer satisfaction surveys;
- Verifying details you have provided, using third party resources (such as psychometric evaluations or skills tests), or to request information (such as references, qualifications and potentially any criminal convictions, to the extent that this is appropriate and in accordance with local laws);
- Complying with our legal obligations in connection with the detection of crime or the collection of taxes or duties; and
- Processing your data to enable us to send you targeted, relevant marketing materials or other communications which we think are likely to be of interest to you.

We may use your personal data for the above purposes if we deem it necessary to do so for our **legitimate interests** (see our legal basis for collecting data – Introduction). If you are not happy with this, in certain circumstances you have the right to object and can find out more about how and when to do in section three.

Marketing Activities

- We may periodically send you information that we think you may find interesting, or to ask for your help with connecting other candidates with jobs. In particular, we may wish to use your data for the purposes listed below, where appropriate and in accordance with any local laws and requirements. Please note that this list is not exhaustive. To:

- enable us to develop and market other products and services;
- market our full range of recruitment services (permanent, temporary, contract, outplacement, MSP programmes and RPO services) to you;
- send you details of reports, promotions, newsletters and market updates, networking and client events, and general information about the industry sectors which we think might be of interest to you;
- display promotional excerpts from your details on Cedar' website(s) as a success story (only where we have obtained your express consent to do so); and
- provide you with information about certain discounts and offers that you are eligible for by virtue of your relationship with Cedar.

- We need your consent for some aspects of these activities which are not covered by our legitimate interests (in particular, the collection of data via cookies, and the delivery of direct marketing to you through digital channels) and, depending on the

situation, we'll ask for this via an opt-in or soft-opt-in (which we explain further below). Please note that in certain of the jurisdictions in which we operate, we comply with additional local law requirements.

- Soft opt-in consent is a specific type of consent which applies where you have previously engaged with us (for example by submitting a job application or CV, or registering a vacancy to be filled), and we are marketing other recruitment-related services. Under 'soft opt-in' consent, we will take your consent as given unless or until you opt out. For most people, this is beneficial as it allows us to suggest other jobs to you alongside the specific one you applied for, significantly increasing the likelihood of us finding you a new position.

- If you are not happy about our approach to marketing, you have the right to withdraw your consent at any time and can find out more about how to do so here. Nobody's perfect, even though we try to be. We want to let you know that even if you have opted out from our marketing communications through our preference centre, it is possible that your details may be recaptured through public sources in an unconnected marketing campaign. We will try to make sure this doesn't happen, but if it does, we're sorry. We'd just ask that in those circumstances you opt out again.

All our marketing is based on what we think will serve our clients and candidates best, but we know we will not always get it right for everyone.

Equal opportunities monitoring and other sensitive personal data

We are committed to ensuring that our recruitment processes are aligned with our approach to equal opportunities. Some of the data we may (in appropriate circumstances and in accordance with local law and requirements) collect about you comes under the umbrella of "diversity information". This could be information about your ethnic background, gender, disability, age, sexual orientation, religion or other similar beliefs, and/or social-economic background. Where appropriate and in accordance with local laws and requirements, we'll use this information on an anonymised basis to monitor our compliance with our equal opportunities policy. We may also disclose this (suitably anonymised where relevant) data to clients where this is contractually required or the client specifically requests such information to enable them to comply with their own employment processes.

- This information is what is called 'sensitive' personal information and slightly stricter data protection rules apply to it. We therefore need to obtain your explicit consent before we can use it. If we need to collect and use this type of information we'll ask for your consent by offering you an opt-in. This means that you have to explicitly and clearly tell us that you agree to us collecting and using this information.

- We may collect other sensitive personal data about you, such as health-related information, religious affiliation, or details of any criminal convictions if this is appropriate in accordance with local laws and is required for a role that you are interested in applying for. We will never do this without your explicit consent.

If you are not happy about this, you have the right to withdraw your consent at any time and you can find out how to do so here.

To help us to establish, exercise or defend legal claims

In more unusual circumstances, we may use your personal data to help us to establish, exercise or defend legal claims.

- **CLIENT DATA:** The main reason for using information about clients is to ensure that the contractual arrangements between us can properly be implemented so that the relationship can run smoothly. This may involve: (i) identifying candidates who we think will be the right fit for you or your organisation; (ii) providing you with an MSP programme (or assisting another organisation to do so); and/or (iii) providing you with RPO services (or assisting another organisation to do so). The more information we have, the more bespoke we can make our service.

We use Client information for:

- Recruitment Activities;
- Marketing Activities; and
- To help us to establish, exercise or defend legal claims.

Recruitment Activities

Our main area of work is recruitment, through: (i) providing you with Candidates; (ii) RPO services; and (iii) MSP programmes. We've listed below the various ways in which we use your data in order to facilitate this.

- Storing your details (and updating them when necessary) on our database, so that we can contact you in relation to recruitment activities;
- Keeping records of our conversations and meetings, so that we can provide targeted services to you;
- Undertaking customer satisfaction surveys; and
- Processing your data for the purpose of targeting appropriate marketing campaigns.

We may use your personal data for these purposes if we deem this to be necessary for our **legitimate interests** (see our legal basis for collecting data – Introduction). If you are not happy with this, in certain circumstances you have the right to object and can find out more about how and when to do in section three.

Marketing Activities

Subject to any applicable local laws and requirements, **we will not**, as a matter of course, seek your consent when sending marketing materials such as our newsletter, market updates, salary surveys/ white papers, candidate CVs or profiles to a corporate postal or email address.

We deem this to be necessary for our **legitimate interests** (see our legal basis for collecting data – Introduction). If you are not happy with this, and would like to withdraw your consent or update your marketing preferences here.

- **SUPPLIER DATA:** The main reasons for using your personal data are to ensure that the contractual arrangements between us can properly be implemented so that the relationship can run smoothly, and to comply with legal requirements.

  We realise that you're probably busy, and don't want us to be contacting you about all sorts of things. To find the right balance, we will only use your information:

  - To store (and update when necessary) your details on our database, so that we can contact you in relation to our agreements;
  - To offer services to you or to obtain support and services from you;
  - To perform certain legal obligations;
  - To help us to target appropriate marketing campaigns; and
  - In more unusual circumstances, to help us to establish, exercise or defend legal claims.

  We may use your personal data for these purposes if we deem this to be necessary for our legitimate interests. If you want to know more about what this means, please click here. We **will not**, as a matter of course, seek your consent when sending marketing messages to a corporate postal or email address. If you are not happy about this, If you are not happy with this, and would like to withdraw your consent or update your marketing preferences here.

- **PEOPLE WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, SUCH AS REFEREES AND EMERGENCY CONTACTS:** We use referees' personal data to help our candidates to find employment which is suited to them. If we are able to verify their details and qualifications, we can make sure that they are well matched with prospective employers. We may also use referees' personal data to contact them in relation to recruitment activities that may be of interest to them. We use the personal details of a candidates or employees emergency contact in the case of an accident or emergency affecting that candidates or employee.

  We will only use the information that our Candidate gives us about you for the following purposes:
  - If our Candidates or Staff members put you down on our form as an emergency contact, we'll contact you in the case of an accident or emergency affecting them; or
  - If you were put down by our Candidate or a prospective member of Staff as a referee, we will contact you in order to take up a reference. This is an important part of our Candidate quality assurance process, and could be the difference between the individual getting a job or not;
  - If you were put down by our Candidate or a prospective employee as a referee, we may sometimes use your details to contact you in relation to recruitment activities that we think may be of interest to you, in which case we will use your data for the same purposes for which we use the data of Clients. If you would like to find out more about what this means, please click here.

  We may use your personal data for these purposes if we deem this to be necessary for our **legitimate interests** (see our legal basis for collecting data – Introduction). If you are not happy with this, and would like to withdraw your consent or update your marketing preferences here.

- **WEBSITE USERS:** We use your data to help us to improve your experience of using our website, for example by analysing your recent job search criteria to help us to present jobs to you that we think you'll be interested in. If you are also a candidate or client of Cedar, we may use data from your use of our websites to enhance other aspects of our communications with, or service to, you. If you would like to find out more about cookies, including how we use them and what choices are available to you, please click here.

  Please note that communications to and from Cedar's employees including emails may be reviewed as part of internal or external investigations or litigation.

  We use your data to help us to improve your experience of using our website, for example by analysing your recent job search criteria to help us to present jobs or candidates to you that we think you'll be interested in. If you would like to find out more about cookies, including how we use them and what choices are available to you, please click here.

SECTION 3: STORAGE & ACCESS

The personal information that you provide to us (including sensitive personal information) may be accessible by the third parties specified above. Some of these companies, clients and third parties are located outside of the European Economic Area. Accordingly your personal information will be sent to or be capable of being accessed from outside the European Economic Area.

When we transfer your personal information outside the European Economic Area we will take steps with the aim of ensuring that your privacy rights continue to be protected as outlined in this Privacy Policy.

HOW DO WE PROCESS & STORE YOUR DATA?

- **CANDIDATE DATA:** Cedar think it's reasonable to expect that if you are looking for employment or have posted your professional CV information on a job board or professional networking site, you are happy for us to collect and otherwise use your personal data to offer or provide our recruitment services to you, share that information with prospective employers and assess your skills against our bank of vacancies. Once it's looking like you may get the job, your prospective employer may also want to double check any information you've given us (such as the results from psychometric evaluations or skills tests) or to confirm your references, qualifications and criminal record, to the extent that this is appropriate and in accordance with local laws. We need to do these things so that we can function as a profit-making business, and to help you and other candidates get the jobs you deserve.

  We want to provide you with tailored job recommendations and relevant articles to read to help you on your job hunt. We therefore think it's reasonable for us to process your data to make sure that we send you the most appropriate content.

  We have to make sure our business runs smoothly, so that we can carry on providing services to candidates like you. We therefore also need to use your data for our internal administrative activities, like payroll and invoicing where relevant.

  We have our own obligations under the law, which it is a legitimate interest of ours to insist on meeting. If we believe in good faith that it is necessary, we may therefore share your data in connection with crime detection, tax collection or actual or anticipated litigation.

- **CLIENT DATA:** To ensure that we provide you with the best service possible, we store your personal data and/or the personal data of individual contacts at your organisation as well as keeping records of our conversations, meetings, registered jobs and placements. From time to time, we may also ask you to undertake a customer satisfaction survey. We think this is reasonable – we deem these uses of your data to be necessary for our legitimate interests as an organisation providing various recruitment services to you.

- **SUPPLIER DATA:** We use and store the personal data of individuals within your organisation in order to facilitate the receipt of services from you as one of our suppliers. We also hold your financial details, so that we can pay you for your services. We deem all such activities to be necessary within the range of our legitimate interests as a recipient of your services.

- **PEOPLE WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, SUCH AS REFEREES AND EMERGENCY CONTACTS:** If you have been put down by a candidate or a prospective employee one of their referees, we use your personal data in order to contact you for a reference. This is a part of our quality assurance procedure and so we deem this to be necessary for our legitimate interests as an organisation offering recruitment services and employing people ourselves.

  If a candidate or employee has given us your details as an emergency contact, we will use these details to contact you in the case of an accident or emergency. We are sure you will agree that this is a vital element of our people-orientated organisation, and so is necessary for our legitimate interests.

HOW LONG DO WE KEEP YOUR PERSONAL DATA FOR?

We will use reasonable endeavours to ensure that your Personal Data is maintained and up to date. However, you are under a duty to inform us of any and all changes to your Personal Data to ensure that it is up to date and we will update or delete your Personal Data accordingly.

- We will delete your personal data from our systems if we have not had any meaningful contact with you (or, where appropriate, the company you are working for or with) for five years (or for such longer period as we believe in good faith that the law or relevant regulators require us to preserve your data). We are required by law to hold your information for as long as is necessary to comply with our statutory and contractual obligations and in accordance with our legitimate interests as a data controller. After this period, it is likely your data will no longer be relevant for the purposes for which it was collected.
- For those candidates whose services are provided via a third party company or other entity, "meaningful contact" with you means meaningful contact with the company or entity which supplies your services. Where we are notified by such company or entity that it no longer has that relationship with you, we will retain your data for no longer than five years from that point or, if later, for the period of five years from the point we subsequently have meaningful contact directly with you.
- For client data, we will delete your personal data from our systems if we have not had any meaningful contact with you (or, where appropriate, the company you are working for or with) for 15 years (or for such longer period as we believe in good faith that the law or relevant regulators require us to preserve your data). We are required by law to hold your information for as long as is necessary to comply with our statutory and contractual obligations and in accordance with our legitimate interests as a data controller. After this period, it is likely your data will no longer be relevant for the purposes for which it

was collected.

When we refer to "meaningful contact", we mean, for example, communication between us (either verbal or written), or where you are actively engaging with our online services. If you are a candidate we will consider there to be meaningful contact with you if you submit your updated CV onto our website. We will also consider it meaningful contact if you communicate with us about potential roles, either by verbal or written communication or click through or replying to any of our marketing communications.

N.B - while we will endeavour to permanently delete your personal data once it reaches the end of its retention period or where we receive a valid request from you to do so, some of your data may still exist within our systems, for example if it is waiting to be overwritten. For our purposes, this data is beyond use, meaning that, while it still exists on an archive system, this cannot be readily accessed by any of our operational systems, processes or employees.

HOW CAN YOU ACCESS, AMEND OR TAKE BACK THE PERSONAL DATA THAT YOU HAVE GIVEN TO US?

One of the GDPR's main objectives is to protect and clarify the rights of EU citizens and individuals in the EU with regards to data privacy. This means that you retain various rights in respect of your data, even once you have given it to us. These are described in more detail below.

If you would like to make a request for information, please contact datacompliance@cedarrecruitment.com. You also have the right to ask Cedar Recruitment Ltd to stop using your information. However, if this involves a request for deletion of your file, please be aware that we may not be required or able to do so, particularly where your file also holds information about our clients or financial information that we need to keep for periods of up to six years or for as long as legally required, i.e. that relate to tax matters for HMRC and Companies House regulations etc. Where we are unable to comply with your request we will provide reasons for failing to do so.

To get in touch about these rights, please contact us on datacompliance@cedarrecruitment.com. We will seek to deal with your request without undue delay, and in any event within one month (subject to any extensions to which we are lawfully entitled). Please note that we may keep a record of your communications to help us resolve any issues which you raise.

Even if we already hold your personal data, you still have various rights in relation to it:

- **Right to object:** this right enables you to object to us processing your personal data where we do so for one of the following four reasons: (i) our legitimate interests outlined above; (ii) to enable us to perform a task in the public interest or exercise official authority; (iii) to send you direct marketing materials; and (iv) for scientific, historical, research, or statistical purposes.

  If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases). Generally, we will only disagree with you if certain limited conditions apply.

  The "legitimate interests" and "direct marketing" categories above are the ones most likely to apply to our website users, candidates, clients and suppliers. If your objection relates to us processing your personal data because we deem it necessary for your legitimate interests, we must act on your objection by ceasing the activity in question unless:

  - we can show that we have compelling legitimate grounds for processing which overrides your interests; or
  - we are processing your data for the establishment, exercise or defence of a legal claim.

  If your objection relates to direct marketing, we must act on your objection by ceasing this activity. You can update your preferences here or by emailing us at datacompliance@cedarrecruitment.com.

- **Right to withdraw consent:** Where we have obtained your consent to process your personal data for certain activities (for example, for marketing), you may withdraw this consent at any time and we will cease to carry out the particular activity that you previously consented to unless we consider that there is an alternative reason to justify our continued processing of your data for this purpose in which case we will inform you of this condition.

  If your interests or requirements change, you can unsubscribe from part or all of our marketing content (for example job role emails or Cedar newsletters) by clicking the unsubscribe link in the email, or by updating your preferences through our preference centre on the Cedar website. You can withdraw your consent, update your preferences here or email us your request at datacompliance@cedarrecruitment.com.

  Data Subject Access Requests (DSAR): You have the right to ask us to confirm what information we hold about you at any time, and you may ask us to modify, update or delete such information. At this point we may comply with your request or, additionally do one of the following:

  - we may ask you to verify your identity, or ask for more information about your request; and
  - where we are legally permitted to do so, we may decline your request, but we will explain why if we do so.

  You can request this by emailing us at datacompliance@cedarrecruitment.com.

- **Right to erasure:** In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. You can request this by emailing us at datacompliance@cedarrecruitment.com. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will delete your data but will generally assume that you would prefer us to keep a note of your name on our register of individuals who would prefer not to be contacted. That way, we will minimise the chances of you being contacted in the future where your data are collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.

  Normally, the information must meet one of the following criteria:

  - the data are no longer necessary for the purpose for which we originally collected and/or processed them;
  - where previously given, you have withdrawn your consent to us processing your data, and there is no other valid reason for us to continue processing;
  - the data has been processed unlawfully (i.e. in a manner which does not comply with the GDPR);
  - it is necessary for the data to be erased in order for us to comply with our legal obligations as a data controller; or
  - if we process the data because we believe it necessary to do so for our legitimate interests, you object to the processing and we are unable to demonstrate overriding legitimate grounds for our continued processing.

  We would only be entitled to refuse to comply with your request for one of the following reasons:

  - to exercise the right of freedom of expression and information;
  - to comply with legal obligations or for the performance of a public interest task or exercise of official authority;
  - for public health reasons in the public interest;
  - for archival, research or statistical purposes; or
  - to exercise or defend a legal claim.

  When complying with a valid request for the erasure of data we will take all reasonably practicable steps to delete the relevant data.

  N.B - while we will endeavour to permanently erase your personal data once it reaches the end of its retention period or where we receive a valid request from you to do so, some of your data may still exist within our systems, for example if it is waiting to be overwritten. For our purposes, this data has been put beyond use, meaning that, while it still exists on an archive system, this cannot be readily accessed by any of our operational systems, processes or employees.

  Right of data portability: If you wish, you have the right to transfer your personal data between data controllers. In effect, this means that you are able to transfer your Cedar account details to another online platform. To allow you to do so, we will provide you with your data in a commonly used machine-readable format that is password-protected so that you can transfer the data to another online platform. Alternatively, we may directly transfer the data for you. This right of data portability applies to: (i) personal data that we process automatically (i.e. without any human intervention); (ii) personal data provided by you; and (iii) personal data that we process based on your consent or in order to fulfil a contract. Do can request this by emailing us at datacompliance@cedarrecruitment.com.

  Data Subject Access Requests (DSAR): You may ask us to confirm what information we hold about you at any time, and request us to modify, update or delete such information. We may ask you to verify your identity and for more information about your request. If we provide you with access to the information we hold about you, we will not charge you for this unless your request is "manifestly unfounded or excessive". If you request further copies of this information from us, we may charge you a reasonable administrative cost where legally permissible. Where we are legally permitted to do so, we may refuse your request. If we refuse your request we will always tell you the reasons for doing so. You can request this by emailing us at datacompliance@cedarrecruitment.com.

- **Right to restrict processing:** You have the right to request that we restrict our processing of your personal data in certain circumstances. This means that we can only continue to store your data and will not be able to carry out any further processing activities with it until either: (i) one of the circumstances listed below is resolved; (ii) you consent; or (iii) further processing is necessary for either the establishment, exercise or defence of legal claims, the protection of the rights of another individual, or reasons of important EU or Member State public interest.

  The circumstances in which you are entitled to request that we restrict the processing of your personal data are:

  - Where you dispute the accuracy of the personal data that we are processing about you. In this case, our processing of your personal data will be restricted for the period during which the accuracy of the data is verified;
  - Where you object to our processing of your personal data for our legitimate interests. Here, you can request that the data be restricted while we verify our grounds for processing your personal data;
  - Where our processing of your data is unlawful, but you would prefer us to restrict our processing of it rather than erasing it; and
  - Where we have no further need to process your personal data but you require the data to establish, exercise, or defend legal claims.

  If we have shared your personal data with third parties, we will notify them about the restricted processing unless this is impossible or involves disproportionate effort. We will, of course, notify you before lifting any restriction on processing your personal data.

You can request this by emailing us at datacompliance@cedarrecruitment.com.

Right to rectification: You also have the right to request that we rectify any inaccurate or incomplete personal data that we hold about you. If we have shared this personal data with third parties, we will notify them about the rectification unless this is impossible or involves disproportionate effort. Where appropriate, we will also tell you which third parties we have disclosed the inaccurate or incomplete personal data to. Where we think that it is reasonable for us not to comply with your request, we will explain our reasons for this decision. It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during the period for which we hold your data.

You can request rectification of your data by emailing us at datacompliance@cedarrecruitment.com. You may ask to unsubscribe from email marketing at any time. Details of how to do so can be found here.

- **Right to lodge a complaint with a supervisory authority:** You also have the right to lodge a complaint with your local supervisory authority.

  If you would like to exercise any of these rights, or withdraw your consent to the processing of your personal data (where consent is our legal basis for processing your personal data), please contact us at datacompliance@cedarrecruitment.com. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

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

  - Phone: 0303 123 1113
  - Email: casework@ico.org.uk
  - Live chat
  - Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

SECTION 4: HOW DO WE SAFEGARD YOUR DATA?

We are committed to taking all reasonable and appropriate steps to protect the personal information that we hold from misuse, loss, or unauthorised access. We do this by having in place a range of appropriate technical and organisational measures. These include measures to deal with any suspected data breach.

If you suspect any misuse or loss of or unauthorised access to your personal information please let us know immediately by contacting Kirsty McBean on 0203 002 8050 or km@cedarrecruitment.com.

We care about protecting your information. That's why we put in place appropriate measures that are designed to prevent unauthorised access to, and misuse of, your personal data.

SENDING US INFORMATION OVER THE INTERNET

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. Therefore, by browsing our website and communicating electronically with us, you acknowledge and agree to our processing of personal data in this way.

Your information is held on servers hosted by us or our Internet Services Provider. 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; any transmission is at your own risk.

SECTION 5: WHO DO WE SHARE YOUR PERSONAL DATA WITH?

Where appropriate and in accordance with local laws and requirements, we may share your personal data, in various ways and for various reasons, with the following categories of people:

- Individuals and organisations who hold information related to your reference or application to work with us, such as current, past or prospective employers, educators and examining bodies and employment and recruitment agencies;
- Tax, audit, or other authorities, when we believe in good faith that the law or other regulation requires us to share this data (for example, because of a request by a tax authority or in connection with any anticipated litigation);
- Third party service providers who perform functions on our behalf (including external consultants, business associates and professional advisers such as lawyers, auditors and accountants, technical support functions and IT consultants carrying out testing and development work on our business technology systems);
- Third party outsourced IT and document storage providers where we have an appropriate processing agreement (or similar protections) in place;
- Marketing technology platforms and suppliers;
- If Cedar merges with or is acquired by another business or company in the future, (or is in meaningful discussions about such a possibility) we may share your personal data with the (prospective) new owners of the business or company.

- In the case of Candidates and our Candidates' and prospective members of Staff's referees: third parties who we have retained to provide services such as reference, qualification and criminal convictions checks, to the extent that these checks are appropriate and in accordance with local laws.

- **CANDIDATE SPECIFIC DATA:** We may share your personal data with various parties, in various ways and for various reasons. Primarily we will share your information with prospective employers to increase your chances of securing the job you want. Unless you specify otherwise, we may also share your information with any of our group companies and associated third parties such as our service providers where we feel this will help us to provide you with the best possible service.
    - potential employers and other recruitment agencies/organisations to increase your chances of finding employment;
    - third party partners, job boards and job aggregators where we consider this will improve the chances of finding you the right job;

- **CLIENT SPECIFIC DATA:** We will share your data: (i) primarily to ensure that we provide you with a suitable pool of candidates; (ii) to provide you with an MSP programme (or assist another organisation to do so); and/or (iii) to provide you with RPO services (or assist another organisation to do so). Unless you specify otherwise, we may share your information with any of our group companies and associated third parties such as our service providers to help us meet these aims.

- **SUPPLIER DATA:** Unless you specify otherwise, we may share your information with any of our group companies and associated third parties such as our service providers and organisations to whom we provide services.

- **PEOPLE WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, SUCH AS REFEREES AND EMERGENCY CONTACTS:** Unless you specify otherwise, we may share your information with any of our group companies and associated third parties such as our service providers and organisations to whom we provide services.
- **WEBSITE USERS:** Unless you specify otherwise, we may share your information with providers of web analytics services, marketing automation platforms and social media services to make sure any advertising you receive is targeted to you.

TO HELP US TO ESTABLISH, EXERCISE OR DEFEND LEGAL CLAIMS

In more unusual circumstances, we may use your personal data to help us to establish, exercise or defend legal claims. Sometimes it may be necessary for us to process personal data and, where appropriate and in accordance with local laws and requirements, sensitive personal data in connection with exercising or defending legal claims. Article 9(2)(f) of the GDPR allows this where the processing "is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity".

This may arise for example where we need to take legal advice in relation to legal proceedings or are required by law to preserve or disclose certain information as part of the legal process.

HOW DO WE TRANSFER YOUR DATA INTERNATIONALLY?

Cedar may operate on an international basis and we may have to transfer or store your data internationally.

- between and within Cedar entities;
- to third parties (such as advisers or other Suppliers to Cedar)
- to overseas Clients;
- to Clients within your country who may, in turn, transfer your data internationally;
- to a cloud-based storage provider; and
- to other third parties, previously referred to.

We want to make sure that your data is stored and transferred in a way which is secure. We will therefore, only transfer data outside of the European Economic Area or EEA (i.e. the Member States of the European Union, together with Norway, Iceland and Liechtenstein) where it is compliant with data protection legislation and the means of transfer provides adequate safeguards in relation to your data, for example:

- by way of data transfer agreement, incorporating the current standard contractual clauses adopted by the European Commission for the transfer of personal data by data controllers in the EEA to data controllers and processors in jurisdictions without adequate data protection laws; or
- by signing up to the EU-U.S. Privacy Shield Framework for the transfer of personal data from entities in the EU to entities in the United States of America or any equivalent agreement in respect of other jurisdictions; or
- transferring your data to a country where there has been a finding of adequacy by the European Commission in respect of that country's levels of data protection via its legislation; or
- where it is necessary for the conclusion or performance of a contract between ourselves and a third party and the transfer is in your interests for the purposes of that contract (for example, if we need to transfer data outside the EEA in order to meet our obligations under that contract if you are a Client of ours); or
- where you have consented to the data transfer.

To ensure that your personal information receives an adequate level of protection, we have put in place appropriate procedures with the third parties we share your personal data with to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the law on data protection.

Consent

- In certain circumstances, we are required to obtain your consent to the processing of your personal data in relation to certain activities. Depending on exactly what we are doing with your information, this consent will be opt-in consent or soft opt-in consent.

- Article 4(11) of the GDPR states that (opt-in) consent is "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." In plain language, this means that:
  - you have to give us your consent freely, without us putting you under any type of pressure;
  - you have to know what you are consenting to – so we'll make sure we give you enough information;
  - you should have control over which processing activities you consent to and which you don't. We provide these finer controls within our privacy preference centre; and
  - you need to take positive and affirmative action in giving us your consent – we're likely to provide a tick box for you to check so that this requirement is met in a clear and unambiguous fashion.

  We will keep records of the consents that you have given in this way.

- We have already mentioned that, in some cases, we will be able to rely on soft opt-in consent. We are allowed to market products or services to you which are related to the recruitment services we provide as long as you do not actively opt-out from these communications.

As we have mentioned, you have the right to withdraw your consent to these activities. You can also update your marketing preferences at any time, and details of how to do so can be found here.

Complaints Policy

Cedar is committed to providing a quality service to our customers. If you are not satisfied with the level of service you have received from us we would like you to tell us about it. All complaints are taken very seriously and all feedback is appreciated as it provides Cedar with an opportunity to improve our standards.

If you would like to make a formal written complaint, you can contact us via email or by post:

Jayne Halperin, Cedar, Floor 2 Goldsmiths House, 137 Regent Street, London W1B 4HZ
E: jayneh@cedarrecruitment.com / howard@cedarrecruitment.com
T: 0203 002 8050

Procedure

1. We will send you written acknowledgement (email or letter), on receipt of your complaint within 5 working days. We will also inform you of the dedicated member of the Quality Care team who will be dealing with your complaint.

2. We will then record your complaints in our central register and start to investigate on your behalf. This is likely to involve the following steps:

Examining your record to ascertain the sequence of relevant events & related correspondence
Interviewing the relevant members of staff for clarification on the issue
Liaising with senior management as appropriate

3. We aim to acknowledge, fully investigate and duly resolve all complaints within 14 working days.

4. A full written response to your complaint will be drafted by the appointed member of the Quality Care team sent to you with supporting documentary evidence (if applicable). In addition, the Quality Care representative may escalate your concerns to the relevant Manager or Director who may wish to discuss the events surrounding your complaint directly with you.

5. If you are not satisfied with the outcome, you can make a written request for escalation of your complaint. The investigation will be reviewed by the team director Kirsty McBean, who will respond directly with her findings and conclusion.

6. If you remain unsatisfied with the decision, you can contact the relevant industry trade association.

Contact

If you have any enquires you can contact us at: info@cedarrecruitment.com or by writing to us at:

Kirsty McBean - Internal Operations Manager
Cedar Recruitment Ltd, Floor 2, Goldsmiths House, 137 Regent Street, London W1B 4HZ

Our registered office is at:

5th Floor, 89 New Bond Street, London W1S 1DA

Change to our Privacy & Complaints Policies

This privacy policy may be changed by Cedar Recruitment Ltd at any time. If we change our privacy policy in the future, we will advise you of changes or updates to our privacy policy by a prominent notice on our website. Continued use of this website or our services after such changes will constitute your acceptance of such changes.

If, at any time, you have questions or concerns about Cedar Recruitment Ltd's privacy commitment, please feel free to e-mail us at datacompliance@cedarrecruitment.com or call 0203 002 8050 to speak to one of our representatives.

GLOSSARY

- **Candidates** – includes applicants for all roles advertised or promoted by Cedar as well as people who have supplied a speculative CV to Cedar not in relation to a specific job. Individual contractors, freelance workers and employees of suppliers or other third parties put forward for roles with Cedar, Clients as part of an MSP offering or otherwise will be treated as candidates for the purposes of this Privacy Policy.

- **Clients** - This category covers our customers, clients, potential future clients and others to whom Cedar provides services in the course of its business.

- **Managed Service Provider (MSP) programmes** – Clients' outsourcing of the management of external staff (including freelance workers, independent contractors and temporary employees) to an external recruitment provider.

- **Employee** – includes employees and interns engaged directly in the business of Cedar (or who have accepted an offer to be engaged) as well as certain other workers engaged in the business of providing services to Cedar (even though they are not classed as employees). For these purposes we also include employees of Cedar who are engaged to work on Clients' premises under the terms of RPO or MSP agreements. To be clear, 'Staff' does not include individuals hired by Cedar for the purpose of being placed with Clients outside of an RPO/MSP arrangement. These individuals are treated in the same way as Cedar' Candidates and are covered by this Privacy Policy. Likewise, independent contractors and consultants performing services for Cedar fall within the definition of a 'Supplier' for the purposes of this Privacy Policy.

- **Suppliers** – refers to partnerships and companies (including sole traders), and atypical workers such as independent contractors and freelance workers, who provide services to Cedar. In certain circumstances Cedar will sub-contract the services it provides to Clients to third party suppliers who perform services on Cedar's behalf. In this context, suppliers that are individual contractors, freelance workers, or employees of suppliers will be treated as Candidates for data protection purposes. Please note that in this context, Cedar requires Suppliers to communicate the relevant parts of this Privacy Policy (namely the sections directed at Candidates) to their employees.

- **Website Users** - any individual who accesses any of the Cedar Recruitment Ltd website.

- Other people whom Cedar may contact – these may include Candidates' and Cedar's Staff emergency contacts and referees. We will only contact them in appropriate circumstances.

APPENDIX 1 – COUNTRY-SPECIFIC VARIATIONS TO OUR PRIVACY POLICY

PRIVACY POLICY TOPIC: CEDAR'S PROCESSING OF YOUR SENSITIVE PERSONAL DATA

JURISDICTION: UK

COUNTRY-SPECIFIC LEGAL REQUIREMENT: Where your personal data are processed in accordance with the fair processing condition relating to our rights and obligations under employment and social security law, this relates to our processing of your personal data which is necessary for compliance with legal obligations (such as ensuring that we pay you statutory sick pay, comply with the statutory employment protections that you enjoy, comply with health and safety laws, and ensure that appropriate National Insurance contributions are made).

P. Data Breach Policy

Causes
Data breaches may be caused by employees, parties external to the organisation, or computer system errors.

Human Error
Human Error causes include:
- Loss of computing devices (portable or otherwise), data storage devices, or paper records containing personal data
- Disclosing data to a wrong recipient
- Handling data in an unauthorised way (e.g.: downloading a local copy of personal data)
- Unauthorised access or disclosure of personal data by employees (e.g.: sharing a login)
- Improper disposal of personal data (e.g.: hard disk, storage media, or paper documents containing personal data sold or discarded before data is properly deleted)

Malicious Activities
Malicious causes include:
- Hacking incidents / Illegal access to databases containing personal data
- Hacking to access unauthorised data via the Coaching App or API
- Theft of computing devices (portable or otherwise), data storage devices, or paper records containing personal data
- Scams that trick Cedar staff into releasing personal data of individuals

Computer System Error
Computer System Error causes include
- Errors or bugs in Cedar' Coaching App, Mobile App, or API
- Failure of cloud services (e.g.: VSTS), cloud computing (e.g.: Azure) or cloud storage (e.g.: Dropbox) security / authentication / authorisation systems

Reporting Breaches
All Cedar employees have an obligation to report actual or potential data protection compliance failures. This allows us to:
- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures

Under the GDPR, Cedar is legally obliged to notify the Supervisory Authority within 72 hours of the data breach (Article 33). Individuals have to be notified if adverse impact is determined (Article 34). In addition, Cedar must notify any affected clients without undue delay after becoming aware of a personal data breach (Article 33).

However, Cedar does not have to notify the data subjects if anonymized data is breached. Specifically, the notice to data subjects is not required if the data controller has implemented pseudonymisation techniques like encryption along with adequate technical and organisational protection measures to the personal data affected by the data breach (Article 34).

Data Breach Team
The Data Breach Team consists of Kirsty McBean, Internal Operations Manager, Anil Bhudia from our IT company, Netflo and Howard Bentwood, CEO. Together, they have the responsibility to make all time-critical decisions on steps taken to contain and manage the incident.

The Data Breach Team should immediately be alerted of any confirmed or suspected data breach via mobile phone in the first instance:

- Kirsty McBean: 07813 978477
- Howard Bentwood: 07977 039 953
- Anil Bhudia: 020 3151 5115
- Email: km@cedarrecruitment.com and/or datacompliance@cedarrecruitment.com.

REPORTING THE INCIDENT TO THE PERSONAL DATA PROTECTION COMMISSION
In the case where affected individuals are in the EU, the relevant supervisory authority must be notified as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals. (Each EU state has its own supervisory authority.)

The notification should include the following information, where available:
- Extent of the data breach
- Type and volume of personal data involved
- Cause or suspected cause of the breach
- Whether the breach has been rectified
- Measures and processes that the organisation had put in place at the time of the breach
- Information on whether affected individuals of the data breach were notified and if not, when the organisation intends to do so

- Contact details of Cedar employees with whom the supervisory authority can liaise for further information or clarification

Where specific information of the data breach is not yet available, Cedar should send an interim notification comprising a brief description of the incident.

Notifications made by organisations or the lack of notification, as well as whether organisations have adequate recovery procedures in place, will affect supervising authorities' decision(s) on whether an organisation has reasonably protected the personal data under its control or possession.

Responding to a Data Breach

DATA BREACH MANAGEMENT PLAN

Upon being notified of a (suspected or confirmed) data breach, the Data Breach Team should immediately activate the data breach & response plan. Cedar' data breach management and response plan is:

1. Confirm the Breach
2. Contain the Breach
3. Assess Risks and Impact
4. Report the Incident
5. Evaluate the Response & Recovery to Prevent Future Breaches

1. CONFIRM THE BREACH
The Data Breach Team (DBT) should act as soon as it is aware of a data breach. Where possible, it should first confirm that the data breach has occurred. It may make sense for the DBT to proceed Contain the Breach on the basis of an unconfirmed reported data breach, depending on the likelihood of the severity of risk.

2. CONTAIN THE BREACH
The DBT should consider the following measures to contain the Breach, where applicable:
Shut down the compromised system that led to the data breach.
Establish whether steps can be taken to recover lost data and limit any damage caused by the breach. (e.g.: remotely disabling / wiping a lost notebook containing personal data of individuals.)

- Prevent further unauthorised access to the system.
- Reset passwords if accounts and / or passwords have been compromised.
- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system.

3. ASSESS RISKS AND IMPACT
Knowing the risks and impact of data breaches will help Cedar determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected.

Risk and Impact on Individuals
- How many people were affected?
  A higher number may not mean a higher risk, but assessing this helps overall risk assessment.
- Whose personal data had been breached?
  Does the personal data belong to employees, customers, or minors? Different people will face varying levels of risk as a result of a loss of personal data.
- What types of personal data were involved?
  This will help to ascertain if there is risk to reputation, identity theft, safety and/or financial loss of affected individuals.
- Any additional measures in place to minimise the impact of a data breach?
  Eg: a lost device protected by a strong password or encryption could reduce the impact of a data breach.

Risk and Impact on Organisations
- What caused the data breach?
  Determining how the breach occurred (through theft, accident, unauthorised access, etc.) will help identify immediate steps to take to contain the breach and restore public confidence in a product or service.
- When and how often did the breach occur?
  Examining this will help Cedar better understand the nature of the breach (e.g. malicious or accidental).
- Who might gain access to the compromised personal data?
  This will ascertain how the compromised data could be used. In particular, affected individuals must be notified if personal data is acquired by an unauthorised person.
- Will compromised data affect transactions with any other third parties?
  Determining this will help identify if other organisations need to be notified.

4. REPORT THE INCIDENT

Cedar is legally required to notify affected individuals if their personal data has been breached. This will encourage individuals to take preventive measures to reduce the impact of the data breach, and also help Cedar rebuild consumer trust.

Who to Notify:

- Notify individuals whose personal data have been compromised.
- Notify other third parties such as banks, credit card companies or the police, where relevant.
- Notify PDPC / GDPR especially if a data breach involves sensitive personal data.
- The relevant authorities (e.g.: police) should be notified if criminal activity is suspected and evidence for investigation should be preserved (e.g.: hacking, theft or unauthorised system access by an employee.)

When to Notify:

- Notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data.
- Notify affected individuals when the data breach is resolved

How to Notify:

- Use the most effective ways to reach out to affected individuals, taking into consideration the urgency of the situation and number of individuals affected (e.g. media releases, social media, mobile messaging, SMS, e-mails, telephone calls).
- Notifications should be simple to understand, specific, and provide clear instructions on what individuals can do to protect themselves.

What to Notify:

- How and when the data breach occurred, and the types of personal data involved in the data breach.
- What Cedar has done or will be doing in response to the risks brought about by the data breach.
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused.
- Contact details and how affected individuals can reach the organisation for further information or assistance (e.g. helpline numbers, e-mail addresses or website).

5. EVALUATE THE RESPONSE & RECOVERY TO PREVENT FUTURE BREACHES

After steps have been taken to resolve the data breach, Cedar should review the cause of the breach and evaluate if existing protection and prevention measures and processes are sufficient to prevent similar breaches from occurring, and where applicable put a stop to practices which led to the data breach.

Operational and Policy Related Issues:

Were audits regularly conducted on both physical and IT-related security measures?

- Are there processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse?
- Were there weaknesses in existing security measures such as the use of outdated software and protection measures, or weaknesses in the use of portable storage devices, networking, or connectivity to the Internet?
- Were the methods for accessing and transmitting personal data sufficiently secure, e.g.: access limited to authorised personnel only?
- Should support services from external parties be enhanced, such as vendors and partners, to better protect personal data?
- Were the responsibilities of vendors and partners clearly defined in relation to the handling of personal data?

Is there a need to develop new data-breach scenarios?

Resource Related Issues:

Were sufficient resources allocated to manage the data breach?

- Should external resources be engaged to better manage such incidents?
- Were key personnel given sufficient resources to manage the incident?

Employee Related Issues:

- Were employees aware of security related issues?
- Was training provided on personal data protection matters and incident management skills?
- Were employees informed of the data breach and the learning points from the incident?

Management Related Issues:

- How was management involved in the management of the data breach?
- Was there a clear line of responsibility and communication during the management of the data breach?

Monitoring

- Everyone at Cedar must observe this policy.
- Cedar has overall responsibility for this policy.
- Cedar will review and monitor this policy regularly to make sure it is effective, relevant, and adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.