Core3 Privacy Policy & Data Protection

April 2022

Introduction

Core3 are committed to protecting the privacy or our clients, candidates and individuals who access our services and website.

This policy applies where we are acting as data controller in regard to the personal data of our candidates and individuals who access our services and website. This means we decide the means and purpose of processing that data.

All organisations that process *personal data* are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their *personal data* whilst imposing certain obligations on the organisations that process their data.

As a recruitment business the Company collects and processes both *personal data* and *sensitive personal data*. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

The security of data is extremely important to our organisation. Core3 take our responsibilities for data compliance very seriously. We have a framework of policies and procedures which ensure that we keep the data we hold on applicants secure.

This policy sets out how the Company implements the Data Protection Laws and protects the privacy of that data.

In this policy the following terms have the following meanings:

'*consent*' means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the *processing* of persona data relating to him or her;

'*data controller*' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the *processing* of *personal data*;

'*data processor*' means an individual or organisation which processes *personal data* on behalf of the *data controller*;

'*personal data*'* means any information relating to an individual who can be identified, such as by 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.

'*personal data breach*' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal data*;

'*processing*' means any operation or set of operations performed on *personal data*, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'*profiling*' means any form of automated *processing* of *personal data* consisting of the use of *personal data* to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'*pseudonymisation*' means the *processing* of *personal data* in such a manner that the *personal data* can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the *personal data* are not attributed to an identified or identifiable individual;

'*sensitive personal data*'* means *personal data* revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the *processing* of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions.

* For the purposes of this policy we use the term '*personal data*' to include '*sensitive personal data*' except where we specifically need to refer to *sensitive personal data*.

'*Supervisory authority*' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the *supervisory authority* is the Information Commissioner's Officer (ICO)

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

Your duty to inform us of changes
Under Data Protection laws it is important that the data we hold is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

The data we collect 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).

We may collect, use, store and transfer different kinds of personal data about you. The type of data we collect about you will depend on your relationship with us. For example, if you are a candidate or client and have requested us to provide work-finding services, if you are a visitor to our website or a subscriber to any of our services.

The Company processes *personal data* in relation to its own staff, work-seekers and individual client contacts and is a *data controller* for the purposes of the Data Protection Laws.

The Company may hold *personal data* on individuals for the following purposes:

- Staff administration;
- Advertising, marketing and public relations please refer to our Marketing Policy
- Accounts and records;
- Administration and *processing* of work-seekers' *personal data* for the purposes of providing work-finding services, including *processing* using software solution providers and back office support
- Administration and *processing* of clients' *personal data* for the purposes of supplying/introducing work-seekers;

Data Retention
The Company will retain your personal data only for as long as is necessary for the purpose we collect it including for the purposes of satisfying any legal, accounting, or reporting requirements. Different laws may also require us to keep different data for different periods of time. For example, the Conduct of Employment Agencies and Employment Businesses Regulations 2003, require us to keep work-seeker records for at least

one year from (a) the date of their creation or (b) after the date on which we last provide you with work-finding services.

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 data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

Your Rights
Please be aware that you have the following data protection rights:

- The right to be informed about the personal data the Company processes on you;
- The right of access to the personal data the Company processes on you;
- The right to rectification of your personal data;
- The right to erasure of your personal data in certain circumstances;
- The right to restrict processing of your personal data;
- The right to data portability in certain circumstances;
- The right to object to the processing of your personal data that was based on a public or legitimate interest;
- The right not to be subjected to automated decision making and profiling; and
- The right to withdraw consent at any time.

Where you have consented to the Company processing your personal data/[and]sensitive personal data you have the right to withdraw that consent at any time by emailing: info@core3.co.uk. We may contact you to clarify your requests so that we may understand your wishes and that we manage your data accordingly. Please note that if you withdraw your consent to further processing that does not affect any processing done prior to the withdrawal of that consent, or which is done according to another legal basis.

There may be circumstances where the Company will still need to process your data for legal or official reasons. Where this is the case, we will tell you and we will restrict the data to only what is necessary for those specific reasons.

If you believe that any of your data that the Company processes is incorrect or incomplete, please contact us using the details above and we will take reasonable steps to check its accuracy and correct it where necessary.

How is your personal data collected?
We may collect your data by the following methods**:**

- **Direct interactions.** You may give us your Identity, Contact details by filling in forms or by corresponding with us by post, phone, and email or otherwise. This includes personal data you provide when you:
    - Enquire or apply for our products or services;
    - create a user account on our website;
    - subscribe to our service or media publications;
    - request any marketing information to be sent to you;
    - take part in a competition, promotion or survey we produce; or
    - provide us with feedback.

- **Automated technologies or interactions.** As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data

about you if you visit other websites employing our cookies. Please see our cookie policy below for further details.

Cookies and how we use them
In order to ensure your website experience is the best it can be we operate certain cookies.
When visiting our website as a first time user, a pop-up cookie message will appear and prompts the user to take positive action to accept cookies. You can opt to accept or decline these cookies.

What do cookies do?

Cookies are used to customize your browsing experience, making it possible to remember your preferences from visit to visit. Thanks to the cookie, our website can present itself at its best to you as a specific user, providing suggestions and inspiration that match your interests and needs based on the preferences you may choose.
Essentially, each cookie is a small lookup table containing pairs of key data values - for example first name and last name. Once the cookie has been read by the code on the server or client computer, data can be retrieved and used to customise the web page appropriately.

If you want to check or change what types of cookies you accept, this can usually be altered within your browser settings.

Why do we use cookies?
The purpose is for the website to be able to recognise you and retain specific information about you. This information may be your login or language preferences etc., so that you don't have to start over on every single visit. Cookie are also used to evaluate Core3 features, develop improvements and conduct business planning, reporting, and forecasting to ensure Core3 provide the best possible service for you.

We use cookies to track your activity to help ensure you get the smoothest possible experience when visiting our website. We can use the information from cookies to ensure we present you with options tailored to your preferences on your next visit. We can also use cookies to analyse traffic and for marketing, promotion, and advertising purposes, including the Facebook Pixel.

What cookies are used on our website?

Third party cookies, Third parties, including Google Analytics and Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from our website and elsewhere on the internet and use that information to provide measurement services and target adverts.

We also use Google Analytics to analyse the use of our website and help us create a more useful and easy to use site. This is a web analytics service provided by Google. Google Analytics uses "cookies", which are text files placed on your computer, to collect information such as visitor numbers and the most popular pages Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, including how to see what cookies have been set and how to manage and delete them, visit http://www.aboutcookies.org or www.allaboutcookies.org. Please note that in a few cases some of our website features may not function if you remove cookies from your browser.

How to control or delete cookies

You have the right to choose whether or not to accept cookies and we have explained how you can exercise this right in the table above. However, please note that if you choose to refuse cookies you may not be able to use the full functionality of our website.

You can block cookies by using the opt-out links provided in the table above, or by changing your browser settings so that cookies from this website cannot be placed on your computer or mobile device. In order to do this, follow the instructions provided by your browser (usually located within the "Help", "Tools" or "Edit" facility). The below hyperlinks provide further guidance on how to disable the use of cookies on certain browsers, and/or on how to delete cookies:

Chrome; Internet Explorer; Safari and Apple support page; Mozilla Firefox; Google Privacy Policy; Chrome web store.

Please note that using a third party opt-out link to disable a cookie or category of cookie may not delete the cookie from your browser but simply disable it from future use. If you wish to delete the relevant cookie, you will need to do this yourself from within your browser.

Links to External website

The Company's website may contains links to other external websites. Please be aware that the Company is not responsible for the privacy practices of such other sites. When you leave our site we encourage you to read the privacy statements of each and every website that collects personally identifiable information. This privacy statement applies solely to information collected by the Company's website.

Data Security

The Company takes every precaution to protect our users' information. Secure Passwords are used for ALL computerised systems. Data is stored on a secure cloud environment within a secure off-site Data Centre located in the UK, with the latest encryption and VPN connectivity and is managed by an external IT services provider to ensure systems and security is managed effectively.

Only employees who need the information to perform a specific job (for example, consultants, our accounts clerk or a marketing assistant) are granted access to your information.

The Company uses all reasonable efforts to safeguard your personal information. However, you should be aware that although we operate a high-level web/mail filtering system the use of email/the Internet is not entirely secure and for this reason the Company cannot guarantee the security or integrity of any personal information which is transferred from you or to you via email/ the Internet.

If you share a device with others we recommend that you do not select the "remember my details" function when that option is offered.

Changes to this Policy

We will update this privacy statement from time to time. We will post any changes on the statement with revision dates. If we make any material changes, we will notify you.

Data Protection

1. The data protection principles

The Data Protection Laws require the Company acting as either *data controller* or *data processor* to process data in accordance with the principles of data protection. These require that *personal data* is:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that *personal data* that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept for no longer than is necessary for the purposes for which the *personal data* are processed;
6. Processed in a manner that ensures appropriate security of the *personal data*, including protection against unauthorised or unlawful *processing* and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and that
7. The *data controller* shall be responsible for, and be able to demonstrate, compliance with the principles.

2. Legal bases for processing

The Company will only process *personal data* where it has a legal basis for doing so (see Annex A). Where the Company does not have a legal reason for *processing personal data* any processing will be a breach of the Data Protection Laws.

The Company will review the *personal data* it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Before transferring *personal data* to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complain and any other third party (such as software solutions providers and back office support)), the Company will establish that it has a legal reason for making the transfer.

a. Legitimate interest

This is where the Company has a legitimate reason to process your data provided it is reasonable and does not go against what you would reasonably expect from us. Where the Company has relied on a legitimate interest to process your personal data our legitimate interests is/are as follows:

- Managing our database and keeping work-seeker and clients records up to date;
- Providing work-finding services to our candidates and clients;
- Contacting you to seek your consent where we need it;
- Giving you information about similar products or services that you have used from us recently;

b. Statutory/contractual requirement

The Company has certain legal and contractual requirements to collect personal data (e.g. to comply with the Conduct of Employment Agencies and Employment Businesses Regulations 2003, immigration and tax legislation, and in some circumstances safeguarding requirements.) Our clients may also require this personal data, and/or we may need your data to enter into a contract with you. If you do not give us personal data we need to collect we may not be able to continue to provide work-finding services to you.

c. Legal Obligation

In some cases we may be required to use your data for the purpose of investigating, reporting and detecting crime and also to comply with laws that apply to us. We may also use your information during the course of internal audits to demonstrate our compliance with certain industry standards.

3. Privacy by design and by default

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all *processing* activities. This includes implementing measures such as:

- data minimisation (i.e. not keeping data for longer than is necessary);
- *pseudonymisation*
- anonymization
- cyber security

For further information please refer to the Company's Information Security Policy.
The Company shall provide any information relating to data *processing* to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The Company may provide this information orally if requested to do so by the individual.

Your Rights in detail

1. Privacy notices
Where the Company collects *personal data* from an individual candidate, the Company will give the individual a privacy notice at the time when it first obtains the *personal data*. This explains in more detail the specific data and information we collect on candidates in order to provide work-finding services.

Where the Company collects *personal data* other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the *personal data*, but at the latest within one month. If the Company intends to disclose the *personal data* to a third party then the privacy notice will be issued when the *personal data* are first disclosed (if not issued sooner). Where the Company intends to further process the *personal data* for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further *processing*.

2. Subject access requests
The individual is entitled to access their *personal data* on request from the *data controller.*

3. Rectification
The individual or another *data controller* at the individual's request, has the right to ask the Company to rectify any inaccurate or incomplete *personal data* concerning an individual.
If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the *personal data* unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

4. Erasure
The individual or another *data controller* at the individual's request, has the right to ask the Company to erase an individual's *personal data.*

If the Company receives a request to erase it will ask the individual if s/he wants his *personal data* to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). The Company cannot keep a record of individuals whose data it has erased so the individual may be contacted again by the Company should the Company come into possession of the individual's *personal data* at a later date.

If the Company has made the data public, it shall take reasonable steps to inform other *data controllers* and *data processors processing* the *personal data* to erase the *personal data*, taking into account available technology and the cost of implementation.

If the Company has given the *personal data* to any third parties it will tell those third parties that it has received a request to erase the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

5. Restriction of *processing*
The individual or a *data controller* at the individual's request, has the right to ask the Company to restrict its *processing* of an individual's *personal data* where:

- The individual challenges the accuracy of the *personal data*;
- The *processing* is unlawful and the individual opposes its erasure;
- The Company no longer needs the *personal data* for the purposes of the *processing*, but the *personal data* is required for the establishment, exercise or defence of legal claims; or
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

If the Company has given the *personal data* to any third parties it will tell those third parties that it has received a request to restrict the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

6. Data portability

The individual shall have the right to receive *personal data* concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another *data controller* in circumstances where:

- The *processing* is based on the individual's *consent* or a contract; and
- The *processing* is carried out by automated means.

Where feasible, the Company will send the *personal data* to a named third party on the individual's request.

7. Object to *processing*

The individual has the right to object to their *personal data* being processed based on a public interest or a legitimate interest. The individual will also be able to object to the *profiling* of their data based on a public interest or a legitimate interest.

The Company shall cease *processing* unless it has compelling legitimate grounds to continue to process the *personal data* which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their *personal data* for direct marketing. Please refer to the Company's Marketing Policy for further information.

8. Enforcement of rights

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision making processes or profiling within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

9. Automated decision making

The Company will not subject individuals to decisions based on automated *processing* that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the *data controller* and the individual;
- Is authorised by law; or
- The individual has given their explicit *consent*.

The Company will not carry out any automated decision-making or *profiling* using the *personal data* of a child.

Reporting *personal data* breaches

All data breaches should be referred to the persons whose details are listed in the Appendix.

1. *Personal data breaches* where the Company is the *data controller*:

Where the Company establishes that a *personal data breach* has taken place, the Company will take steps to contain and recover the breach. Where a *personal data breach* is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

Where the *personal data breach* happens outside the UK, the Company shall alert the relevant *supervisory authority* for data breaches in the effected jurisdiction.

2. *Personal data breaches* where the Company is the *data processor*: The Company will alert the relevant *data controller* as to the *personal data breach* as soon as they are aware of the breach.

3. Communicating *personal data breaches* to individuals

Where the Company has identified a *personal data breach* resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.
The Company will not be required to tell individuals about the *personal data breach* where:

- The Company has implemented appropriate technical and organisational protection measures to the *personal data* affected by the breach, in particular to make the *personal data* unintelligible to any person who is not authorised to access it, such as encryption.
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

The Human Rights Act 1998

All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with *personal data* these should be respected at all times:

- Right to respect for private and family life (Article 8).
- Freedom of thought, belief and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

Complaints

If you have a complaint or suggestion about the Company's handling of *personal data* then please contact the person whose details are listed in the Appendix to this policy.
Alternatively you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

APPENDIX

Access & Responsibility
The following individuals have the following access and responsibility:

- Adding and amending *personal data* – all employees of Core3. In order to carry out the duties of their employment and provide work finding services to individuals and respond to clients' requirements, all staff will require access to the CRM – all have received full GDPR training. Financial data relating payroll and client invoicing data is restricted to the Finance Team and Directors.
- Responding to subject access requests/requests for rectification, erasure, restriction data portability, objection and automated decision making processes and profiling – Managing Director: Leo Hewett. To ensure a strict process is followed limited authority is permitted to the relevant persons named.
- Reporting data breaches/dealing with complaints - Managing Director: Leo Hewett

ANNEX A

a) The lawfulness of *processing* conditions for *personal data* are:

1. *Consent* of the individual for one or more specific purposes.
2. *Processing* is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract
3. *Processing* is necessary for compliance with a legal obligation that the controller is subject to.
4. *Processing* is necessary to protect the vital interests of the individual or another person.
5. *Processing* is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the *data controller*.
6. *Processing* is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of *personal data*, in particular where the individual is a child.

b) The lawfulness of *processing* conditions for *sensitive personal data* are:

1. Explicit *consent* of the individual for one or more specified purposes, unless reliance on *consent* is prohibited by EU or Member State law.
2. *Processing* is necessary for carrying out data controller's obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.
3. *Processing* is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving *consent*.
4. In the course of its legitimate activities*, processing* is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body, with a political, philosophical, religious or trade union aim and on condition that the *processing* relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the *consent* of the individual.
5. *Processing* relates to *personal data* which are manifestly made public by the individual.
6. *Processing* is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
7. *Processing* is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.
8. *Processing* is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.
9. *Processing* is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.
10. *Processing* is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.

This Policy was last updated 03rd March 2022 – effective 04th March 2022