

INTRODUCTION

This Privacy Policy applies to the personal data of our website users, candidates, customers, providers and others who may be contacted by us for further information about our candidates or who have been designated as an emergency contact. It also applies to emergency contacts of our staff.

Please note that we may change this Privacy Policy from time to time. If you wish to keep up to date, please visit our website where we post any changes.

If you are dissatisfied with any aspect of our Privacy Policy, you may have rights, which we have also described in relevant places.

Definitions

- **Candidates** – includes candidates for all positions offered or promoted by Master Care, including permanent, part-time and temporary employment and freelance positions with Master Care customers; as well as individuals who have submitted a CV without reference to a specific job offer. Individual contractors, freelancers and provider employees or other third parties offered positions with Master Care customers under an MSP or other offer shall be treated as candidates for the purposes of this Privacy Policy.
- **Customers** – includes our customers and others to whom Master Care provides services in the course of conducting its business.
- **Delete** – although we shall endeavour to permanently delete your personal data at the end of the data retention period or at your reasonable request, some of your data may still appear on our systems, for example if we need to retain it in accordance with overarching legal regulations. For our purposes, this data may be deactivated, which means that although it will still appear in our archive system, it will not be readily accessible to any of our operating systems, processes or staff.
- **General Data Protection Regulation (GDPR)** – a European Union statutory instrument that aims to harmonise European data protection legislation. Its effective date is 25 May 2018 and any reference to it should be interpreted accordingly to include any national legislation implementing it.
- **Managed Service Provider (MSP) programmes** - the outsourcing of the management of external staff by a customer (including freelancers, independent contractors and temporary workers) to an external recruitment provider.
- **Other individuals we may contact** – may include emergency contacts and reference contacts of Master Care candidates and staff. These people will only be contacted in appropriate circumstances.
- **Recruitment Process Outsourcing (RPO) services** – the full or partial outsourcing of the recruitment process of permanent employees to a recruitment provider.

- **Personnel** – includes employees directly employed by Master Care (or those who have accepted an offer of employment), as well as those providing services to Master Care under civil law contracts. For these purposes, we also include Master Care employees who are engaged to work at Customer sites under the terms of RPO or MSP contracts. For clarity, 'Personnel' does not include individuals employed by Master Care for the purpose of being engaged to work at Customer sites outside of an RPO/MSP contract. These individuals are treated in the same way as Master Care Candidates and are covered by this Privacy Policy. Similarly, independent contractors and consultants providing services to Master Care fall within the definition of 'Provider' for the purposes of this Privacy Policy.
- **Providers** – includes sole traders, partnerships, commercial law companies as well as personal providers such as independent contractors and freelancers who provide services to Master Care. In certain circumstances, Master Care shall subcontract the services provided to Customers to third-party providers who perform services on behalf of Master Care. In this context, providers who are individual contractors, freelancers or employees of providers shall be treated as candidates for data protection purposes. Please note that Master Care requires Providers to communicate the relevant parts of this Privacy Policy (namely the parts directed to candidates) to their employees.

GENERAL PART

What type of personal data do we collect?

CANDIDATE DATA:

In order to provide the best possible employment opportunities tailored to your needs, we need to process certain information about you. We only ask for data that actually help us match the offer to your needs, i.e. for example your first name and surname, age, contact details, education, employment history, emergency contacts, immigration status, financial information (in case we need to verify your financial status) and national insurance number. You may also provide us with other relevant information. In appropriate cases and in accordance with local laws and requirements, we may also collect information about your health or criminal record.

CUSTOMER DETAILS:

If you are a customer of Master Care, we need to collect and use information about you or people in your organisation in the course of providing services to you such as:

- finding candidates suitable for you or your organisation;
- providing you with a managed service provider programme (or supporting another organisation to do so);
- providing you with process outsourcing services (or supporting another organisation to do so);
- notifying you of content published by Master Care that may be relevant and useful to you.

PROVIDER DETAILS:

We need a small amount of information from our providers to make sure our partnership runs smoothly. We need contact details of the right people in your organisation so we can communicate with you. We also need other information, such as your bank account details, so that we can pay you for the services provided (if this is part of the contractual arrangement between us).

PERSONS WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, FOR EXAMPLE REFERENCE CONTACTS AND EMERGENCY CONTACTS:

In order to provide candidates with suitable employment opportunities in a safe manner and to prepare for any eventuality for them and our staff, we need some basic background information. We only ask for very basic contact details so that we can contact you for references or when you have been named as an emergency contact by one of our candidates or members of staff.

CANDIDATE DATA:

We collect your personal data in two ways:

1. Directly from you.
2. From third parties.

CUSTOMER DETAILS:

We collect your personal data in two ways:

1. Directly from you
2. From third parties (for example, our candidates) and from other limited sources (for example, online and other media).

PROVIDER DETAILS:

We collect your personal data in the course of our cooperation.

PERSONS WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, FOR EXAMPLE REFERENCE CONTACTS AND EMERGENCY CONTACTS:

We only collect your contact details if a candidate or a member of our staff mentions you as their emergency contact or the candidate provides them to us as a reference contact.

CANDIDATE DATA:

The main purpose of using your personal data is to help us find you employment or another job that is suitable for you. The more information we have about you, your skills and ambitions, the better we can tailor our service. Where appropriate and in accordance with local laws and requirements, we may also use your personal data for purposes such as marketing and profiling. Where appropriate, we will ask for your consent to undertake some of these activities.

CUSTOMER DETAILS:

The main purpose of using customer information is to make sure that contractual arrangements between us can be properly implemented so that the relationship runs smoothly. These may include:

- finding candidates that we think will be suitable for you or your organisation; and/or;
- providing you with services; and/or
- providing you with outsourced recruitment or managed services (or supporting another organisation to do so). The more information we have, the better we can tailor our service.

PROVIDER DETAILS:

The main purpose of using your personal data is to make sure that the contractual arrangements between us can be properly implemented so that the relationship runs smoothly, and to meet legal requirements.

PERSONS WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, FOR EXAMPLE REFERENCE CONTACTS AND EMERGENCY CONTACTS:

We use the personal data of reference contacts to help our candidates find suitable employment for them. If we can verify their details and qualifications, we can make sure they are a good match for potential employers. We may also use the personal data of reference contacts to contact them in relation to recruitment activities that may be of interest to them. We use the personal data of emergency contacts of a candidate or member of staff in the event of an accident or emergency affecting the candidate or member of staff.

Please note that communications from and to Master Care staff, including e-mails, may be scrutinised as part of internal or external investigations or legal proceedings.

With whom do we share your personal data?

CANDIDATE DATA:

We shall share your personal data with the potential employer for the purposes of which the recruitment in question is being carried out and with entities authorised by law. Provided you have given your consent, we shall share your data with other potential employers in order to increase your chances of obtaining your dream job.

CUSTOMER DETAILS:

We share your data in order to:

- provide you with a suitable pool of candidates;
- provide you with an MSP programme (or support another organisation to do so); and/or
- providing you with RPO services (or supporting another organisation to do so). Unless you choose otherwise, we may share your information with any of our group companies and associated third parties, such as our service providers, for these purposes.

PROVIDER DETAILS:

Unless you choose otherwise, we may also 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.

PERSONS WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, FOR EXAMPLE REFERENCE CONTACTS AND EMERGENCY CONTACTS:

Unless you choose otherwise, we may also 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.

How do we protect your personal data?

We have implemented appropriate technical and organisational measures to ensure that the personal data we process is protected in a manner appropriate to the risks against, for example, unauthorised access, taking by an unauthorised person, processing in breach of data protection legislation and internal regulations, and alteration, loss, damage or destruction.

How long do we store your personal data?

If we have not had significant contact with you (or the company you work for or with) for a period of two years, we will delete your personal data from our systems, unless we are required by law to retain it (for example, for obligations to tax authorities or in connection with any anticipated legal proceedings).

How do you access, correct or withdraw the personal data you have provided to us?

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

- **Right to object:** If we use your data because we consider it necessary for our legitimate interests, which you do not agree with, you have the right to object. We shall respond to your request within 30 days. In some cases we may be entitled to extend this period.
- **Right to withdraw consent:** Once you have given us consent to process your personal data for the purposes of certain activities, e.g. profiling your suitability for certain positions or consenting to marketing to you, you can withdraw your consent at any time.
- **Data subject requests for data:** For the avoidance of doubt - you have the right at any time to ask us to confirm what information we hold about you and you can request that we amend, update or delete such information. At this point, we may comply with your request, or additionally ask you to verify your identity or provide additional information regarding your request, and refuse your request where permitted by law, giving reasons for our decision.
- **Right to delete:** In some situations, e.g. in the case of unlawful processing of your data, you have the right to request the deletion of your personal data. We shall respond to your request within 30 days. In some cases we may be entitled to extend this period.
- **Right to data portability:** You have the right at your discretion to transfer your data from us to another controller. We shall assist you with this - either by directly transferring your data for you, or by providing you with copies in a commonly used machine-processable format.
- **Right to lodge a complaint with a supervisory authority:** You have the right to lodge a complaint with the locally competent supervisory authority.

If your interests or requirements change, you can unsubscribe from some or all of our marketing content, for example, e-mail notifications about announcements or Master Care newsletters.

How do we store and transfer your data abroad?

Master Care operates within the EU, which enables us to offer our services in EU markets. In order for us to continue to operate in this way, it may be necessary to transfer or store your data abroad.

SPECIFIC PART

What type of personal data do we collect?

Are you looking for a bit more information about what data we collect about you? Here you can find more details about the information we may collect. The information described below is, of course, additional to any personal data that we are obliged to process by law.

CANDIDATE DATA:

Depending on applicable laws and requirements, we may collect some or all of the information listed below to enable us to offer you employment opportunities or to keep you employed. In some national jurisdictions, we have restrictions on the processing of the data listed below:

- first name and surname;
- age / date of birth;
- birth certificate;
- gender;
- photography;
- marital status;
- contact details;
- education;
- employment history;
- emergency contacts and details of dependents;
- reference contact details;
- immigration status (when a work permit is required);
- nationality / citizenship / place of birth;
- copy of driving license and/or passport/ID;
- financial information (if we need to verify your financial status);
- social security number (or equivalent in your country) and other tax information;
- information such as racial or ethnic origin, religious beliefs or worldview, mental or physical health conditions, including disability information;
- criminal record information, if required for the position you wish to apply for;
- details of your current salary, pension and employment benefits;
- information about your interests and needs for future employment, collected directly and indirectly, for example from the job offers you view or articles you read on our website;
- additional information that you choose to provide to us;
- additional information that your reference contacts choose to provide to us;
- additional information that our customers may give us about you or that we obtain from external sources, such as job search sites;

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

DATA:

In general, we only need your contact details or the contact details of people in your organisation (i.e. their names, telephone numbers and e-mail addresses, position) in order to ensure efficient contact between us. We also hold information about your online activity within candidate profiles and other material published by Master Care, which we use to ensure that the marketing correspondence you receive are relevant and timely. In some circumstances, such as interactions with finance and collections teams, our conversations with you may be recorded depending on local laws and requirements. If we require additional personal data for any reason, we shall notify you.

PROVIDER DETAILS:

We collect such details of our contacts within your organisation as names, telephone numbers and e-mail addresses. We also collect bank account details for the purpose of transferring remuneration. In some circumstances, such as interactions with finance and collections teams, our conversations with you may be recorded depending on laws and requirements. In addition, we process data resulting from specific legislation e.g. tax legislation.

PERSONS WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, FOR EXAMPLE REFERENCE CONTACTS AND EMERGENCY CONTACTS:

An emergency contact is someone we call in the event of an emergency. In order to ask for references, we obviously need the reference contact's contact details (first name and surname, e-mail address and telephone number). We shall also need this data if our candidate or a member of our staff has listed you as their emergency contact so that we can contact you in the event of an accident or emergency.

How do we collect your personal data?

CANDIDATE DATA:

We collect Candidate personal data in two main ways:

1. Personal data that you provide to us as a candidate;
2. Personal information we obtain from other sources.

Personal data provided by you:

- Master Care needs to know certain information about you in order to provide you with a customised job offer.

You can provide us with information in a number of different ways at your discretion:

- Entering your details on the Master Care website via the application form as part of the registration process;
- Leaving a printed version of your CV at a recruitment event, job fair or at the Master Care office;
- Emailing your CV to a Master Care consultant or undergoing an interview;

- Applying for positions through a job search engine, which redirects you to the Master Care website;

Personal information we obtain from other sources:

We also obtain personal data of candidates from other sources. Depending on the relevant circumstances and applicable laws and requirements, this may include personal data obtained in the following situations:

- Your reference contacts may disclose your personal information;
- Our customers may share your personal information with us;
- We may obtain information about you by searching for potential candidates from external sources, such as LinkedIn and other job search sites;
- If you have liked our Facebook page, Instagram or you follow us on LinkedIn, we receive your personal information from these sites;
- If you have been referred to us by an RPO or MSP provider, they may share your personal information with us.

CUSTOMER DETAILS:

We collect Customer personal information in two ways:

1. Personal data that we receive directly from you.
2. Personal information we obtain from other sources.

Personal data that we receive directly from you.

We have a common goal - to provide the best staff for your organisation. We will receive data directly from you in **two ways**:

1. if you contact us proactively, usually by phone or email.
2. If we contact you, either by phone, email or through our consultants' business development activities.

Personal information we obtain from other sources:

Where appropriate and in accordance with laws and requirements, we may seek additional information about you or your associates from other sources, generally as part of due diligence or market research, including:

1. From market research carried out by a third party and from online and other media analysis that we may carry out ourselves or contract with another organisation to carry out.
2. From lists of attendees at significant events.
3. From other limited sources and from third parties, such as our candidates to the extent that they provide us with your data as their reference contact.

How do we use your personal data?

CANDIDATE DATA:

We generally use candidate data in four ways:

1. Recruitment activities;
2. Marketing activities;
3. To help us establish, exercise or defend legal claims.
4. We may also use candidate data for Profiling in appropriate circumstances in the future.

Below is more information on each of them:

Recruitment activities

The main area of our activity is recruitment - connecting the right candidates with the right positions. We have listed below the different ways we use your personal data for this purpose, where appropriate and in line with legislation and requirements, in particular:

- collecting your data from you and from other sources, for example LinkedIn;
- storing (and updating where necessary) your data in our database so that we can contact you regarding recruitment;
- providing our recruitment services and improving the recruitment process;
- assessing data about you for places of work that we think may be suitable for you;
- sending your information to customers to apply for positions or assess your qualifications;
- enabling you to submit your CV, apply for positions online or subscribe to alerts for jobs that may be of interest to you;
- enabling you to participate in specialised online training courses;
- enabling you to take advantage of the interactive features of our websites;
- fulfilling our obligations under any contracts entered into between us;
- fulfilling our obligations under any contracts entered into between Master Care and third parties in relation to your recruitment;
- streamlining our payroll and invoicing processes;
- carrying out customer satisfaction surveys;
- verifying the data you provide using external resources (such as psychometric testing or aptitude tests) or requests for information (such as references, qualifications and potentially criminal records, to the extent appropriate and in accordance with the law);
- fulfilling our legal obligations in connection with the detection of a crime or the collection of taxes or duties;
- processing your data to enable us to send you selected, relevant marketing material or other correspondence that may be of interest to you;

We may use your personal data for the above purposes where we consider it necessary for our legitimate interests.

Marketing activities

We may need your data for the purposes listed below in particular where it is appropriate in accordance with the law and includes:

- enabling us to develop and market other products and services;
- marketing our full range of recruitment services (temporary and permanent jobs, contracts, career reorientation process, MSP programmes and RPO services);
- sending you details of reports, promotions, offers, networking and customer events, as well as general information about industries that may be of interest to you;
- displaying promotional snippets of your information on Master Care websites as a success story (only with your explicit consent); and
- providing you with information about certain discounts and offers to which you are entitled as a result of your relationship with Master Care.

We need your consent for some aspects of these activities that do not fall under legitimate interests and, depending on the situation, we shall ask you for your consent under on an opt-in or soft opt-in basis (explained below).

Soft opt-in consent is a specific type of consent that applies where you have previously engaged with us in an activity (for example, by submitting an application or CV or registering a vacancy) and we are selling other recruitment services. Under soft opt-in consent, we will consider your consent to have been given until you object. For most people, this is beneficial as it allows us to suggest other positions to you in addition to the one you have applied for, significantly increasing the likelihood of finding you a new job. For other types of online marketing, we are required to obtain your explicit consent to help us establish, exercise or defend legal claims and profiling.

Currently, all of our recruitment activities involve human decision-making, however, in the future we will use automated technologies such as expert systems or machine learning to carry out the candidate selection process from start to finish in appropriate cases and in accordance with the law.

Where appropriate, we will ask for your consent to undertake some or all of these activities. If you do not consent to profiling, your application will still be manually reviewed for the positions you apply for, but your profile will not automatically be considered for other positions. This may reduce the likelihood of finding a position for you.

You have the right to withdraw this consent at any time.

With whom do we share your personal data?

Where appropriate and in accordance with the law and requirements, we may share your personal data, with entities in the following categories:

- individuals and organisations who hold information relating to your reference or application for employment with us, such as current, prospective or potential employers, educational institutions and examination bodies and employment and placement agencies;

- tax, audit and other authorities where we are required by law or other regulation to share this data (for example, at the request of a tax authority or in connection with any anticipated legal proceedings);
- third party providers who perform functions on our behalf (including external consultants, business partners and professional advisors such as lawyers, auditors and accountants, technical support staff and IT consultants testing and developing our business technology systems);
- third-party providers of outsourced IT and document storage services if we have entered into an appropriate contract to outsource the processing of personal data;
- marketing technology platforms and providers;
- in the case of candidates: potential employers and other recruitment agencies/organisations to enhance your chances of finding employment;
- in the case of candidates: third-party partners, portals and job search engines if this improves your chances of finding you the right position;
- in the case of candidates: MSP providers within our Customers' MSP programmes;
- in the case of candidates and reference contacts of our candidates and prospective staff members: third parties that we have retained to provide services such as reference, qualification and criminal record verifications, to the extent that these verifications are appropriate and lawful;
- if Master Care merges or is acquired by another company in the future, (or is in relevant discussions about such a possibility), we may share your personal data in accordance with the new (potential) owners of the company in accordance with the law.

How do we protect your personal data?

We have implemented appropriate technical and organisational measures to ensure that the personal data we process is protected in a manner appropriate to the risks against, for example, unauthorised access, taking by an unauthorised person, processing in breach of data protection legislation and internal regulations, and alteration, loss, damage or destruction.

How long do we store your personal data?

We will delete your personal data from our systems if we have had no significant contact with you (or the company you work for or with) for a period of two years (or for such longer periods if we are required by law or other relevant regulations to retain your data).

For candidates whose services are provided through an external company or other entity, 'significant contact' with you means significant contact with the company or entity that provides your services. In the event that we are notified by such a company or entity that the relationship with you has ceased, we shall retain your data for a period of up to two years from the point at which contact

ceased or (if later) for a period of two years from the point at which we made direct relevant contact with you.

By 'significant contact' we mean, for example, communication between us (oral or written) or your active use of our online services. If you are a candidate, we shall count as meaningful contact if you submit an updated CV to our website or attend any online training. We shall also count as significant contact if you contact us about potential positions, either verbally or in writing, or click through to our marketing correspondence. Your receipt, opening and reading of an e-mail or other digital message does not count as significant contact except in the case of a series of clicks or a direct response.

How do you access, correct or withdraw the personal data you have provided to us?

- **Right to object:** this right allows you to object to our processing of your personal data if we do so for any of the following reasons: (i) our legitimate interests; (ii) to enable us to carry out a task in the public interest or as part of the activities of public authorities; (iii) to send you direct marketing materials; and (iv) for scientific, historical, research or statistical purposes.
- The above categories of 'legitimate interests' and 'direct marketing' most often apply to our website users, candidates, customers and providers. If your objection relates to our processing of your personal data because we consider it necessary for your legitimate interests, we must comply with your objection by ceasing the activities in question unless:
 - we can demonstrate that we have compelling legitimate grounds for the processing that outweigh your interests; or
 - we process your data for the purposes of establishing, exercising or defending a legal claim.
- If your objection relates to direct marketing, we must comply with your objection by ceasing these activities.
- **Right to withdraw consent:** If we have received consent from you to process your personal data for the purposes of certain activities, e.g. marketing arrangements or automated profiling, you may withdraw your consent at any time and we will cease to carry out the activity to which you previously consented, unless there is another basis for further processing of your data, which we will notify you of.
- **Data subject requests for data:** You may at any time ask us to confirm what information we hold about you and request that we amend, update or delete such information. We may ask you to verify your identity and to provide us with additional information regarding your request. If we provide you with the information we hold about you, we will not charge you for this unless your request is 'manifestly unfounded or excessive'. If you request additional copies of this information from us, we may charge you reasonable administrative costs, where permitted by law. We may refuse your request

if the law allows us to do so. If we refuse your request, you shall always know the reasons for our decision.

- **Right to deletion:** you have the right to request the deletion of your data. The information must usually meet the following criteria:

- the data is no longer necessary for the purposes for which it was originally collected and/or processed;
- if you have previously given your consent for us to process your data, you have withdrawn it and there is no other basis for us to continue the processing;
- your data has been processed unlawfully (i.e. in a way that does not comply with data protection legislation, including the GDPR);
- it is necessary to delete the data in order for us to comply with our legal obligations as a data controller; or
- if we process data for our legitimate interests, you object to the processing and we are unable to demonstrate legitimate reasons for further processing.

- Complying with a legitimate request for deletion, we shall take all reasonably feasible measures to delete the relevant data.

- **Right to restrict processing:** In certain circumstances, you have the right to request that we restrict our processing of your data. This means that we may continue to store your data and will not be able to carry out any further processing activities only until:

- the cessation of one of the circumstances listed below;
- you have given your consent; or
- the need for further processing either for the establishment, exercise or defence of legal claims, the protection of another person's rights, or for reasons of substantial EU or Member State public interest.

The circumstances in which you are entitled to request a restriction of the processing of your personal data are as follows:

- you challenge the accuracy of personal data about you that we process. In this case, our processing of your personal data will be limited to the period during which the correctness of the data shall be verified;
- you object to our processing of your personal data in our legitimate interest. In this case, you can request a restriction of your data while we review our basis for processing your personal data;
- if our processing of your data is unlawful, but you prefer that we restrict our processing of your data instead of deleting it; and;
- if there is no longer a need to process your personal data but you need the data to establish, exercise or defend legal claims.

If we have shared your personal data with third parties, we shall notify them of the restriction on processing unless it is impossible or requires a disproportionate effort. We shall, of course, notify you before imposing any restriction on the processing of your personal data.

- **Right to correction:** You also have the right to request that we correct any inaccurate or incomplete personal data that we hold about you. If we have shared this personal data with third parties, we shall notify them of the corrections, unless this is impossible or requires disproportionate effort. Where appropriate, we shall notify you to which third parties we have disclosed incorrect or incomplete personal data. If we do not comply with your request, we shall explain to you the reasons for our decision.
- **Right to data portability:** You have the right, at your discretion, to transfer your personal data between controllers. This means that you can transfer your Master Care account data to another online platform. To enable you to do this, we shall transfer your data in a commonly used machine-processable, password-protected format so that you can transfer your data to another online platform. We may also transfer your data directly to you. The right to data portability applies to:
 - personal data processed automatically (i.e. without any human intervention);
 - personal data provided by you; and
 - personal data that we process on the basis of your consent for the execution of the contract.
- **The right to lodge a complaint** with a supervisory authority in accordance with local jurisdiction. If you wish to exercise any of these rights or withdraw your consent to the processing of your personal data (if consent is our legal basis for processing your personal data), information on how to contact us can be found here. Please note that we may store your correspondence to help us resolve any issues you raise.

You can unsubscribe from the announcement notifications at any time.

It is important that we keep your personal information correct and up to date. Please let us know if your personal data changes during the period we process it.

How do we store and transfer your data abroad?

In order to provide you with the best possible service and to fulfil the purposes described in this Privacy Policy, your data may be transferred:

Pursuant to Articles 44-49 of the GDPR, we shall transfer data outside of the European Economic Area or EEA (the Member States of the European Union plus Norway, Iceland and Liechtenstein) if it complies with data protection legislation and the means of transfer provide adequate protection for your data, for example:

- through a data transfer contract containing the current standard contractual clauses adopted by the European Commission;
- by transferring your data to a country where the European Commission has made a determination of the adequacy of the level of data protection in such country through its legislation;

- if it is necessary for the conclusion or performance of a contract between us and a third party and the transfer is in your interest for the purposes of the contract (if, for example, we need to transfer your data outside the EEA in order to fulfil our contractual obligations if you are our Customer); or
- if you have consented to the transfer of your data.

Legal basis for processing your data

LEGITIMATE INTEREST

Pursuant to Article 6(1)(f) of the GDPR, we may process your data where this is 'necessary for the purposes of the legitimate interests pursued by [us] or by a third party, except where these interests are overridden by [your] interests or fundamental rights and freedoms, requiring the protection of personal data'.

CANDIDATE DATA:

We believe it is a reasonable expectation that if you are looking for a job or have posted your CV on a job search site or social media site specialising in professional networking, you do not mind us collecting or otherwise using your personal information to offer you or provide you with recruitment services, share this information with potential employers and verify your skills in relation to our vacancy database. When it looks like you will be hired, your prospective employer may also want to verify the information you have provided to us (such as the results of psychometric or aptitude tests), or confirm your references, qualifications or criminal record information to the extent that these verifications are appropriate and legally compliant.

We want to provide you with individually customised position recommendations and relevant articles to help you in your job search process. We therefore believe that it is legitimate for us to process your data in order to ensure that we send you the most appropriate content.

We need to ensure that our business runs smoothly so that we can continue to provide services to candidates like you. Where appropriate, we therefore also need to use your data for our internal administrative activities such as payroll and invoicing.

We have our own legal obligations which we have a legitimate interest in fulfilling! If we consider it necessary in good faith, we may share your data in connection with criminal prosecution, tax collection and actual or anticipated prosecution or court proceedings.

CUSTOMER DETAILS:

In order to provide you with the best possible service, we keep your personal data and/or the personal data of your organisation's contacts, as well as documentation of our conversations, meetings, registered positions and places of work. We may periodically ask you to complete a customer satisfaction survey. We consider this to be a legitimate activity - we consider the above uses of your data to be necessary for our legitimate interests as an organisation providing a variety of recruitment services to you.

PROVIDER DETAILS:

We use and hold data about individuals within our organisation to improve the perception of services from you as one of our providers. We also hold financial data so that we can pay you for your services. We consider all such activities necessary as part of our legitimate interests as a consumer of your services.

PERSONS WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, FOR EXAMPLE REFERENCE CONTACTS AND EMERGENCY CONTACTS:

- if our candidate or prospective member of staff has listed you as a reference contact, we shall use your details to contact you for a reference. This is part of our quality assurance process, so we consider it necessary for our legitimate interests as an organisation offering recruitment and staffing services;
- if a candidate or member of staff has given us your details as an emergency contact, we shall use these details to contact you in the event of an accident or emergency. We are sure you agree that this is an important part of our people-focused organisation and therefore necessary for our legitimate interests.

CONSENT

In certain circumstances we are required to obtain your consent to process your personal data in connection with certain activities. Depending on exactly what we are doing with your information, this consent shall be given on an opt-in or soft opt-in basis.

Article 4(11) of the GDPR states that consent means 'a freely given, specific, informed and unequivocal demonstration of intent by which the data subject, by means of a statement or a clear affirmative action, consents to the processing of personal data relating to them'.

In simple terms, this means that:

- you must give us your consent voluntarily, without us exerting any pressure on you;
- you need to know what you are agreeing to, so we shall make sure we have given you sufficient information;
- you must take a positive and affirmative action in giving us your consent - we can provide a box to tick to make this requirement clear and unambiguous.

We shall record the consents that have been given in this way.

As mentioned, in some cases we shall be able to rely on soft opt-in consent. We may sell you products or services related to the recruitment services we provide, unless you object to receiving such correspondence. You have the right to withdraw your consent to the above at any time.

ESTABLISHMENT, EXERCISE OR DEFENCE OF LEGAL CLAIMS

Sometimes it may be necessary for us to assert or defend against claims, in which case we may process your personal data until the conclusion of the pending proceedings and until the expiry of the limitation period for claims against you, which is 3 years (Article 118 of the Civil Code), and in

specific situations provided by law, this period may be longer. Article 6(2)(f) of the GDPR allows for the above i.e. in our legitimate interest of pursuing or defending against your claims.

The above circumstances may, for example, occur if we need legal advice in connection with legal proceedings or if the law requires the retention or disclosure of certain information as part of a legal process.

How to contact us?

- For all matters that relate to our processing of your personal data;
- In order for us to exercise your rights under the GDPR: to access your data, to obtain a copy of your data, to rectify your data, to restrict the processing of your data, to restrict the transfer of your data, to object and to withdraw your consent (if a consent is the legal basis for our processing of your personal data);

If you wish to exercise these rights you should contact us and let us know which right and to what extent you wish to exercise it.

You may also contact us with any comments or suggestions regarding this Privacy Policy.

You can write to us at the following address:

ul. Postępu 15C

02-676 Warsaw, Poland

E-mail:

iod@mastercare.pl

Tel.:

+48 696-499-064

How to contact your local supervisory authority?

Country where you use or provide services to Master Care: Poland

Details of your supervisory authority:

Personal Data Protection Office - you can contact it in the following way:

Address:

ul. Stawki 2,

00-193 Warsaw, Poland

Tel.:

(+48) 22 531 03 00

Fax:

(+48) 22 531 03 01

E-mail:

kancelaria@uodo.gov.pl