FUSION Associates

Last update: 16/07/18

Privacy Policy (candidates/clients/source/referees/suppliers/users of website)

If you're looking for information about how to have your details removed, updated or disclosed to you from Fusion Associates, 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 0207 856 0071 or dpo@fusionassociates.eu.

WHO WE ARE

We are Fusion WDT Limited and we represent the businesses that trade as Fusion Associates. Further information about our firm can be found by clicking here.

Fusion WDT Ltd (trading as Fusion Associates), 76 Woodcock Hill, Harrow, Middlesex, HA3 0JD or contacted on 0207 856 0070.

Fusion WDT Ltd is registered under the Information Commissioner's Office. Registration Number: **ZA045990.**

Fusion Associates ("we", "us") is committed to keeping your information secure and managing it in accordance with our legal responsibilities, under the privacy and data protection laws applicable wherever we operate in the world, as well as the General Data Protection Regulation (Regulation (EC) 2016/679 ("GDPR") in the European Union ("EU")).

We keep this Privacy Policy under regular review and update it from time to time. This policy was last updated in May 2018. Please review this policy periodically for any changes.

This Privacy Policy (together with our Terms & Conditions) sets out the basis on which all personal data that we collect from you, or that you provide to us directly and via our websites listed below will be processed by us:

www.fusionassociates.eu
www.fusionassociates.de
www.fusionassociates.fr
www.fusionassociates.es
www.fusionassociates.it
www.fusionassociates.co.uk

WHO THIS POLICY APPLIES TO

We provide executive search, assessment and leadership services and the provision of interim managers ("our services") to a range of clients throughout the world. Details of our services can be found elsewhere on this website or those listed above. This policy applies to you whether you are a candidate for one of our clients, an individual we are assessing as an employee of one of our clients, a client or whether you are a source or a referee in respect of a candidate or an employee of one of our clients. Additionally, this policy will apply to you if you attend one of our events or have subscribed to receive information about our services and/or our newsletter.

For the purposes of this policy:

- candidate(s) means an individual who is a candidate, applicant, potential candidate, employee of a client;
- client(s) means any, business, firm, organisation, government body or individual that mandates us to perform any of our services;
- a referee is a person who provides a personal or work reference in respect of a candidate and;
- a source is a person who provides us with information or intelligence about a candidate.
- A supplier is a firm who provides us with services to operate our business.

GATHERING INFORMATION

Our clients expect that we identify the best individuals to fill roles within their organisations. So, we need to research systems, online databases and other information sources, and talk to many individuals. Besides our clients, these will include referees and sources to help inform our decision-making process.

The nature of our work means we are required to process personal data quickly, confidentially and often without reference to the data subject. Accordingly, we process such data in accordance with the Data Protection Laws, regularly using our legitimate interest where it is not possible or feasible to speak directly with the data subject. Beyond this, we will seek consent in the circumstances explained later in this policy document.

We collect information from candidates directly when you upload your CV or resume via our Career page or when you send this to us via email or post. We also collect information from you when you speak with a Fusion Associates employee anywhere around the world.

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.

Fusion WDT Ltd (trading as Fusion Associates) 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 Fusion'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."

- Fusion 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 open roles
- To enable you to submit your CV and apply online for jobs.
- 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, interim, contract)
- 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

Fusion 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 Fusion website or via an application form, as part of the registration process;
- Leaving a hard copy CV with a Fusion consultant when meeting them in person;
- Emailing your CV to a Fusion consultant or being interviewed by them;

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, XING and other networking or 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;
- At trade fairs;
- 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 job or for consideration by our consultants for positions as they arise. Your CV will be stored in the Fusion Associates CRM, and will be accessible by Fusion's employees in the UK and abroad. You can update your CV at any time, simply by following the same procedure to submit a new CV. Your old CV will be archived during our periodical data purging process, 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 'contact us' form, 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 – or more specifically Executive Search (head hunting), identifying, evaluating and providing our clients with suitable candidates for open roles we are managing exclusively for them. 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, XING;
- 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;
- Sending Progress Reports to Clients in order to provide clients with a summary of who we have been interviewing, screening and evaluating when working on a recruitment mandate.
- Enabling you to submit your CV
- Carrying out our obligations arising from any contracts entered into between us;
- Carrying out our obligations arising from any contracts entered into between Fusion and third parties in relation to your recruitment;
- 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 range of recruitment services (permanent, interim, contract) to you;
- send you details of reports, 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 testimonial excerpts from your details on Fusion' website(s) as a success story (only where we have obtained your express consent to do so)

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) 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). 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

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.

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.

PEOPLE WHOSE DATA WE RECEIVE FROM CANDIDATES AND STAFF, SUCH AS SOURCES, 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. As well as basic contact information we will also collect information regarding your credentials as a source, details of your relationship/knowledge of a candidate and your opinions of that individual. We may obtain this information directly from you or publicly available information.

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

WEBSITE USERS: We use your data to help us to improve your experience of using our website, for example by understanding which blog posts are more popular helps us determine what future blog posts to write. If you are also a candidate or client of Fusion, 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 Fusion's employees including emails may be reviewed as part of internal or external investigations or litigation.

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: Fusion think it's reasonable to expect that if you are looking for employment or have posted your professional CV information on a professional networking site (like XING or Linkedin), 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 current list of job 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 seven 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 seven years from that point or, if later, for the period of seven 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 dpo@fusionassociates.eu. You also have the right to ask Fusion Associates 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 dpo@fusionassociates.eu. 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 from any marketing emails or by emailing us at dpo@fusionassociates.eu

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 our marketing content by clicking the ‘unsubscribe’ link in the email. You can withdraw your consent here.

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:

If your interests or requirements change, you can unsubscribe from our marketing content by clicking the ‘unsubscribe’ link in the email. You can withdraw your consent here.

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 dpo@fusionassociates.eu

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 dpo@fusionassociates.eu. 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 Fusion 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. You can request this by emailing us at dpo@fusionassociates.eu.

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 dpo@fusionassociates.eu

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 dpo@fusionassociates.eu.

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 dpo@fusionassociates.eu. You may ask to 'unsubscribe' from email marketing at any time.

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 dpo@fusionassociates.eu. 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

- 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 Alex Pescott on 0207 856 0071 or alex@fusionassociates.eu.

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 (for example Mailchimp) and suppliers;
- If Fusion 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 recruitment partners in the USA, Nordics and Asia

CLIENT SPECIFIC DATA: We will share your data: (i) primarily to ensure that we provide you with a suitable pool of candidates; (ii) and/or 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?

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

- between and within Fusion entities;
- to third parties (such as advisers or other Suppliers to Fusion)
- 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.
- 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 via one of our marketing emails.

Complaints Policy

Fusion Associates 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 Fusion with an opportunity to improve our standards.

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

Alex Pescott (CEO)
E: alex@fusionassociates.eu
T: 0207 856 0071

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 DPO (Data Protection Officer) 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

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 DPO sent to you with supporting documentary evidence (if applicable).

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 Partners of the business and one of them will respond directly with their findings and conclusion.

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

Contact

If you have any enquiries you can contact us at: info@fusionasscociates.eu

Our registered office is at:

Fusion Associates, 76 Woodcock Hill, Harrow, Middlesex, HA3 0JD

Change to our Privacy & Complaints Policies

This privacy policy may be changed by Fusion Associates 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 Fusion Associates's privacy commitment, please feel free to e-mail us at dpo@fusionassociates.eu or call 0207 856 0070 to speak to one of our representatives.

GLOSSARY

- **Candidates** – includes applicants, potential candidates and employees of a client who have engaged with Fusion Associates regarding career opportunities either advertised or promoted by Fusion as well as people who have supplied a speculative CV to Fusion not in relation to a specific job. Individual contractors, freelance workers and employees of suppliers or other third parties put forward for roles with Fusion, 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 Fusion provides services in the course of its business.

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

- **Employee** – includes employees and interns engaged directly in the business of Fusion (or who have accepted an offer to be engaged) as well as certain other workers engaged in the business of providing services to Fusion (even though they are not classed as employees). To be clear, 'Staff' does not include individuals hired by Fusion for the purpose of being placed with Clients outside of an RPO/MSP arrangement. These individuals are treated in the same way as Fusion' Candidates and are covered by this Privacy Policy. Likewise, independent contractors and consultants performing services for Fusion 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 Fusion. In certain circumstances Fusion will sub-contract the services it provides to Clients to third party suppliers who perform services on Fusion'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, Fusion requires Suppliers to communicate the relevant parts of this Privacy Policy (namely the sections directed at Candidates) to their employees.

- **A referee** – is a person who provides a personal or work reference in respect of a candidate

- **A source** – is a person who provides us with information or intelligence about a candidate.

- **Website Users** - any individual who accesses any of the Fusion Associates websites.

- **Other people whom Fusion may contact** – these may include Candidates' and Fusion'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: FUSION'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).

A. 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 Fusion staff into releasing personal data of individuals

Computer System Error
Computer System Error causes include
- Errors or bugs in Fusion's website, specifically the career form (which uses JotForm)
- Failure of cloud computing (e.g.: Remote Desktop Protocol) or cloud storage (e.g. OneDrive) security / authentication / authorisation systems

Reporting Breaches
All Fusion 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, Fusion 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, Fusion must notify any affected clients without undue delay after becoming aware of a personal data breach (Article 33).

However, Fusion 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 Alex Pescott (Fusion Associates), Simon Ponsford from our IT company Tivarri and Spencer Jeffries at Accelerator (our email exchange server). 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:

- Alex Pescott: 0207 856 0071
- Email: alex@fusionassociates.eu and/or dpo@fusionassociates.eu.

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 Fusion employees with whom the supervisory authority can liaise for further information or clarification

Where specific information of the data breach is not yet available, Fusion 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. Fusion' 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 Fusion 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 Fusion 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
Fusion 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 Fusion 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 Fusion 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, Fusion 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 Fusion must observe this policy.
- Fusion has overall responsibility for this policy.
- Fusion 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.