Data Processing Agreement (DPA)

This Data Processing Agreement ("DPA") is entered into between Techfellow Limited ("Techfellow") and the Customer, Client or Supplier and is incorporated into and governed by our Terms & Conditions of Business or Consultancy Services Agreement. This DPA specifically incorporates the main service provision of recruitment or consultancy services ("Services").

1. DPA Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Terms & Conditions of Business or in the Consultancy Services Agreement.

"Client" or means a customer, client or supplier business that have entered into an agreement under Terms & Conditions of Business or Consultancy Services Agreement with Techfellow for the provision of the Services.

"Controller" means Techfellow (or Client of);

"Terms and Conditions "means the agreement between Techfellow and Client for the provision of the Services;

"Data Subject" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (as amended from time to time, or replaced by subsequent legislation);

"DPA" means this data processing agreement together with associated documentation;

"Personal Data" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (as amended from time to time, or replaced by subsequent legislation);

"Processor" means Techfellow and in many instances the Client;

"Sub-Processor" means any person or entity engaged by us (including a Subsidiary) to process Personal Data in the provision of the Services to the Client.

2. Purpose

The Processor has agreed to provide the Services to the Controller in accordance with the Terms and Conditions. In providing the Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA. Both Techfellow and Client will each be acting as separate Data Controllers and Data Processors in respect of the Data provided in the provision of Services. Whether acting as a Data Controller or a Data Processor, the Processor will comply with the provisions of Data Protection Law, and in particular the GDPR in the collection, storage and Processing of the Data provided.

3. Scope

In providing the Services to the Controller pursuant to the Terms and Conditions, the Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with both the Terms and Conditions and the Controller's instructions documented in the Terms and Conditions and this DPA.

4. Processor Obligations

The Processor may collect, process or use Personal Data only within the scope of this DPA.

The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach any applicable data protection laws.

The Processor confirms that it shall process Personal Data on behalf of the Controller and shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process the Personal Data except on instructions from the Controller

The Processor shall ensure that all employees, agents and officers involved in the handling of Personal Data:

(i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

The Processor shall implement appropriate technical and organisational procedures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

The technical and organisational measures detailed in the associated documentation shall be at all times adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA provided that such updates and modifications do not result in the degradation of the overall security of the Services.

Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data.

5. Controller Obligations

The Controller represents and warrants that it shall comply with the Terms and Conditions, this DPA and all applicable data protection laws.

The Controller represents and warrants that it has obtained any and all necessary permissions and authorisations necessary to permit the Processor, its Subsidiaries and Sub-Processors, to execute their rights or perform their obligations under this DPA.

The Controller is responsible for compliance with all applicable data protection legislation, including requirements with regards to the transfer of Personal Data under this DPA and the Terms and Conditions.

All Subsidiaries of the Controller who use the Services shall comply with the obligations of the Controller set out in this DPA.

The Controller has their own obligations to implement their own appropriate technical and organisational procedures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to

Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

The Controller shall take steps to ensure that any natural person acting under the authority of the Controller who has access to Personal Data does not process the Personal Data except on instructions from the Controller.

The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Terms and Conditions. The Processor will process the request to the extent it is lawful, and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

The Controller acknowledges and agrees that some instructions from the Controller, including destruction or return of data from the Processor, may result in additional fees. In such case, the Processor will notify the Controller of such fees in advance unless otherwise agreed.

6. Sub-Processors

The Controller acknowledges and agrees that:

(i) Subsidiaries of the Processor may be used as Sub-processors; and

(ii) the Processor and its Subsidiaries respectively may engage Sub-processors in connection with the provision of the Services.

All Sub-processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor similar to those set out in this DPA.

Where Sub-processors are located outside of the EEA, the Processor confirms that such Sub-processors:

(i) are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or

(ii) have entered into Standard Contractual Clauses with the Processor; or

(iii) have other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

The Processor shall make available to the Controller the current list of Sub-processors which shall include the identities of Sub-processors and their country of location. During the term of this DPA, the Processor shall provide the Controller with at least 30 days prior notification, via email (or in-application notice), of any changes to the list of Sub-processor(s) who may process Personal Data before authorising any new or replacement Sub-processor(s) to process Personal Data in connection with the provision of the Services.

If the Controller objects to a new or replacement Sub-processor the Controller may terminate the Terms and Conditions with respect to those Services which cannot be provided by the Processor without the use of the new or replacement Sub-processor. The Processor will refund the Controller any prepaid fees covering the remainder of the Term of the Terms and Conditions following the effective date of termination with respect to such terminated Services.

7. EU Data Subject's Data Transferred outside of the EEA

Where Personal Data relating to an EU Data Subject is transferred outside of the EEA it shall be processed only by entities which:

(i) are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or

(ii) have entered into Standard Contractual Clauses with the Processor; or

(iii) have other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

8. Liability

The limitations on liability set out in the Terms and Conditions apply to all claims made pursuant to any breach of the terms of this DPA. The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Terms and Conditions.

The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Subsidiaries as if such acts, omissions or negligence had been committed by the Controller itself. The Controller shall not be entitled to recover more than once in respect of the same claim.

9. Audit

The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

Any audit conducted under this DPA shall consist of an examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Terms and Conditions. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may at its own expense conduct a more extensive audit which will be:

(i) limited in scope to matters specific to the Controller and agreed in advance with the Processor;

(ii) carried out during UK business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and

(iii) conducted in a way which does not interfere with the Processor's day-to-day business. The Processor may charge a fee (based on its reasonable time and costs) for assisting with any audit. The Processor will provide the Controller with further details of any applicable fee, and the basis of its calculation, in advance of any such audit.

This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

10. Data Deletion and Retention

The parties agree that on the termination of the provision of Services, the Processor and the Sub-Processor shall, at the choice of the Controller, return all Personal Data transferred and the copies thereof to the Controller or shall delete (or anonymise as directed) all the Personal Data and certify to the Controller that it has done so, unless legislation imposed upon the Processor prevents it from returning or deleting all or part of the Personal Data transferred. In that case, the Processor warrants that it will guarantee the confidentiality or the Personal Data and will not actively process the Personal Data transferred anymore.

The Processor and the Sub-Processor warrant that upon request of the Controller and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to.

Notification of Data Breach

The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data ("Data Breach").

The Processor will take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Data Breach and to assist the Controller in meeting the Controller's obligations under applicable law.

The Processor's notification of, or response to, a Data Breach under this Section 11 will not be construed as an acknowledgement by the Processor of any fault or liability with respect to the Data Breach.

The Processor will not assess the content of the Controller's data in order to identify information subject to any specific Controller data breach. The Controller is solely responsible for complying with data breach notification laws applicable to the Controller and fulfilling any third party notification obligations related to any Data Breach(es).

12. Compliance, Cooperation and Response

In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request or assisting the Controller in complying with its duties. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable.

The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller unless such notification is not permitted under applicable law or a relevant court order.

The Processor may make copies of and/or retain Personal Data in order to comply with its legal or regulatory requirement including, but not limited to, retention requirements.

The parties acknowledge that it is the duty of the Controller to notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the parties agree that amendments are required, but the Processor is unable to accommodate the necessary changes, the Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.

The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a supervisory data protection authority in the performance of their respective obligations under this DPA.

The parties agree that the Processor will be entitled to charge the Controller additional fees to reimburse the Processor for its staff time, costs and expenses in assisting the Controller, when the Controller requests the Processor to provide assistance pursuant to this DPA. In such cases, the Processor will notify the Controller of its fees for providing assistance, in advance.

13. Term and Termination

The term of this DPA shall coincide with the commencement of the Terms and Conditions and this DPA shall terminate automatically together with termination or expiry of the Terms and Conditions.

14. General

This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

This DPA shall be governed by the laws of England and Wales. The courts of England and Wales shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

Data Protection/Security:

Data security policy

This policy outlines behaviours expected of employees when dealing with data and provides a classification of the types of data with which they should be concerned.

Techfellow Ltd must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting its customers. The protection of data in scope is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. Its primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

Scope

These measures must be applied to all protected personal or otherwise sensitive data. Protected personal data is defined at Annex A and is any material that links an identifiable individual with information whose release would put them at significant risk of harm or distress. It also covers any source of information relating to 1,000 or more individuals that is not in the public domain, even if the information about an individual is not considered likely to cause harm or distress.

- During the course of business the Company may hold personal data relating to individuals. The General Data Protection Regulation (GDPR) requires the Company to maintain strict security in relation to personal data held by it relating to individuals whether those individuals are clients or suppliers, or prospective clients or suppliers, or prospective employees;
- No information referring to private individuals should be taken or sent from the Company's offices and each employee must understand the importance of not divulging any such information to persons other than other employees within the Company. Employees asked to transfer personal data to recipients outside the Company (e.g. giving out a home telephone number of an employee or details of a customer) should satisfy themselves that the transfer is authorised by the Company before carrying out such a request;
- Employees should be aware that it is a criminal offence to access or disclose personal data held by the Company without authority;
- Employees who have access to or control over personal data held by the Company, e.g. employee records/lists or details relating to customers or private individuals, should ensure that access to the data within the Company is restricted on a need to know basis and that it is stored in accordance with the data security provisions set out below;
- Protected Personal Data (as defined in Annex A) which is held on paper must be locked away when not in use and offices in which it is held must be secured;
- All computers (whether remote or otherwise) are password protected, configured so that functionally is minimised to it's intended business use only, and have up to date software patches and anti-virus software;
- All material that has been used for protected data should be subject to controlled disposal;
- All laptops, drives or removable electronic data media containing personal data should be encrypted. Laptops and drives or any other removable electronic media containing protected personal data are to be held in locked cabinets or drawers when not in use;
- It is company policy that protected personal data may not be transferred to third party owned laptops, PCs, USB keys, external drives and any other removable electronic media;
- As part of the Company's terms and conditions of employment, employees consent to the Company holding and using personal data relating to them. Personal data includes names and addresses, bank details, health records and most of the information that it needs to hold about employees for employment purposes. On joining Techfellow Ltd, the employee will be required to notify the Company of such personal details. Any relevant changes to such personal information must be notified to the management;
- For the purposes of the General Data Protection Regulation (GDPR), the Company needs to specify the purposes for which we will use that information. The Company will of course only use it for legitimate purposes. Those purposes include:

    - Complying with obligations to its employees. It needs personal data so it can perform activities such as contacting and paying employees, and complying with its obligations under health and safety regulations;
    - Assessing employees, their performance and suitability for particular roles;
    - Doing anything for the benefit of welfare of employees, their families and dependants;
    - Complying with its obligations under the general law, e.g. in relation to taxation, social security, or law enforcement;
    - Providing information about employees to those who require it in connection with services that they provide to it or we to them, or who do or may own the Company or who may need it in connection with the assumption by them of responsibility for any of its employees (e.g. in outsourcing arrangements);
    - The prosecution or defence of any legal proceedings
- Information risk management: The data protection measures outlined in this policy are to be implemented through the following processes:
    - Initial induction training for all staff;
    - Regular refresher training for all staff, as required;
    - Publication of data protection policy in the staff handbook as well as quarterly risk assessments.

Annex A

Definition of protected personal data

As a minimum, personal data includes all data falling into either category A or B below:-

A: Any information that links one or more identifiable living person with private information about them

There should be protection for a data set that includes:-

- One or more of the pieces of information through which an individual may be identified (name, address, telephone number, driving licence number, date of birth, photograph etc.), combined with;
- Information about that individual whose release could case harm or distress, including:-
    - DNA or finger prints;
    - Bank/financial/credit card details;
    - National Insurance number;
    - Passport number/information on immigration status;
    - Travel details (for example at immigration control, or Oyster records);
    - Tax, benefit or pension records;
    - Place of work;
    - School attendance/records;
    - Conviction/prison/court records/evidence;
    - Groups/affiliations/political or other sensitive personal data as defined by the GDPR.

Note: this is not an exhaustive list.

B: Any source of information about 1,000 identifiable individuals or more, other than information sources from the public domain.

Note that this is a minimum standard. Information on smaller numbers of individuals may justify protection because of the nature of the individuals, source of the information, or extent of information.

Data Subject Rights (& controlling your personal information)

The General Data Protection Regulation (GDPR) provides the same rights as those under the DPA but provides you with some significant enhancements. In addition to the policies and procedures to ensure individuals can enforce their data protection rights, we offer to provide individual's right to access any personal information that Techfellow processes about them and to request information about:

- what personal data we hold about them
- the purposes of the processing
- the recipients to whom the personal data has/will be disclosed
- how long we intend to store their personal data for
- if we did not collect the data directly from them, information about the source
- the right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- the right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- the right to lodge a complaint and who to contact in such instances

We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so. We may use your personal information to send you promotional information about third parties which we think you may find interesting if you tell us that you wish this to happen.

Subject Access Request (SAR)

We have put in place procedures to accommodate the 30-day timeframe for providing the requested information. We will provide, in an intelligible form, copies of the personal data and any information about the sources of the data. If we believe that the request is excessive, in terms of an unreasonable amount of historical data, we may refuse with a clear explanation. We will not charge for an audit report. As above, you have the right at any time to require us to update, modify or delete any personal information which we hold about you.

GDPR FAQ'S

1) What is GDPR?

The General Data Protection Regulation is a European-wide law that replaces the Data Protection Act 1998. It strengthens and unifies data protection, changing the legal basis for collection and processing of personal data, applying stricter requirements for consent. It places greater obligations on how organisations handle and process personal data.

2) Who does GDPR affect?

GDPR affects every business and applies in all EU member states as (of 25 May 2018). It also affects businesses outside the EU who process the personal data of EU residents and offer them goods and services, irrespective of whether payment is required; or where the processing by a business relates to the monitoring of the behaviour of EU residents in so far as their behaviour takes place within the EU.

3) Does Brexit matter?

The UK is implementing a new Data Protection Bill which largely includes all the provisions of the GDPR.

4) How does Techfellow enforce GDPR?

Techfellow has always taken the protection, privacy and security of your data very seriously. When GDPR was introduced, we reviewed our systems, processes and procedures to ensure we were fully compliant by May 25, 2018. For example we:

- updated all of our electronic systems increasing data integrity, confidentiality and availability.
- introduced a new Data Processing Agreement which we and you agree to undertake (as of May 25, 2018 onwards).
- updated our Privacy Policy to empower you to make the best decisions about the information you share with us, and to ensure our compliance in respect of the data we hold about you.
- made all our consent mechanisms clear and understandable.

5) What information does GDPR apply to?

GDPR applies to 'Personal Data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This applies to both automated personal data and to manual filing systems.

6) How long will you keep my data?

Where you have provided your consent, we will only retain your personal data for the lawful basis for our recruitment processing activity, the provision of:

- work-finding services.
- suitable professionals to employ.
- professional services under a contract for services.

We will not use your personal data for an unrelated process, therefore we will keep your data until such time that you decide to exercise your right to withdraw consent and decide to have your personal data erased. We may refuse to comply with a request for erasure where personal data is processed to comply with a legal obligation or official authority.

7) What is Subject Access Request (SAR)?

Individuals (Data Subjects) have a right to be informed by an organisation whether or not it is processing personal data that relates to them and, if so, to be told:

- what personal data it is processing.
- the purposes for which the personal data is being processed.
- who, if anyone, the personal data is disclosed to.

- the extent to which it is using the personal data for the purpose of making automated decisions relating to the data subject and, if so, what logic is being used for that purpose.

Techfellow are required to respond to an SAR by providing, in an intelligible form, copies of the personal data and any information about the sources of the data. We have a month to respond to the request. If we believe that the request is excessive, in terms of an unreasonable amount of historical data, we may refuse with a clear explanation. We will not charge for an audit report.

8) What data will you keep relating to me?

We are required to retain certain information for audit, legal and compliance purposes. The data retained will be your name and job title, contact information including email address, Curriculum Vitae information and data, demographic information such as postcode, preferences and interests, and any other information relevant to our recruitment processing activity.

9) Do you have a nominated Data Protection Officer (DPO)?

Our DPO is Paul Redman, his contact email is dpo@techfellow.co.uk. The DPO is responsible for promoting awareness of the GDPR across the organisation, continued assessment of our GDPR policies and procedures, identifying any gap areas and implementing the new policies, procedures and measures.

Information Security Statement:

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect. We use Microsoft Azure to host our systems, applications and data; Microsoft leads the industry in establishing clear security and privacy requirements and then consistently meeting these requirements. Azure meets a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia IRAP, UK G-Cloud and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate.

All Techfellow Ltd employees are instructed to follow a firm-wide security policy. Only authorised personnel are provided access to personally-identifiable information and these employees are required to agree to ensure confidentiality of this information. Any paper-based personal data, such references, shall be viewable and securely stored by relevant staff who need access to such data.