**Data Protection Supplier Risk Assessment**

|  |  |  |
| --- | --- | --- |
|  **General Information**  | ***Examples*** | **Response** |
| **1** | Please list the different types of personal data which will be exchanged with APM and the purpose for providing the data. | *Individual’s first name**Individual’s surname**Individual’s home address* |  |
| **2** | What is the postal address for the premises from which the data is processed? Please confirm if your organisation owns these premises. |  |  |
| **3** | What is the name and telephone number of your company’s Information Security or Data Protection Manager?  |  |  |
| **4** | Is your company registered with the Information Commissioner’s Office? If yes, what is your registration number?  |  |  |
| **5** | Please list all sub-contractors you will use to process candidate data, and the steps taken to ensure their compliance with data protection requirements. | *Contractual clauses**Reviews of security controls* |  |
|  **Physical Security** | **Response** |
| **6** | Describe the security measures in place to protect APM’s information on your premises and how any electronic backups of data will be secured.  |  |
| **Technical Controls** | ***Examples*** | **Response** |
| **7** | Does the company have information security procedures for protecting its systems against the vulnerabilities of unauthorised or unlawful processing and against accidental loss or destruction of damage to data? If so, please provide details | *Limited and controlled user access to systems**Password controls**Server security**Retention periods**Staff and contractor data protection training* |  |
| **Operating System Security** | ***Examples*** | **Response** |
| **8** | What security measures will be used to safeguard the data when in transit to APM? | *Secure FTP* *Password protection**Encryption* |  |
| **9** | Please list all countries in which you will process data before forwarding to APM and the country in which data will be processed when returned to you by APM (if different).  | *Where information is held electronically please confirm the country or territory where your server is located.*  |  |
| **Organisational Standards** | **Response** |
| **10** | What practices does your company follow for disposing of sensitive written or printed material? |  |
| **11** | Does your company have procedures for reporting security incidents to your clients? Is information security or data protection training mandatory for your staff? |  |
| **Human Resources Security** | **Response** |
| **12** | Has your company self-reported or been reported for any information security incidents (theft, misuse, losses) to the Information Commissioner’s Office in the last 3 years? If so please describe the incident(s) and the outcome.  |  |

***I confirm that the information I have provided on this questionnaire is true and accurate to the best of my ability.***

Company:

Print name:

Position:

Signature:

Date: