## Supplier data and security questionnaire

### Data Protection Officer

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| What is the name and contact details of your Data Protection Officer? | Charles Dickinson – charles.dickinson@peoplehr.com |

### Accreditations

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| What security accreditations you have? | ISO27001 |

### Systems and applications

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Where is your data centre location? | Slough, UK |
| Will the space in your data centre be shared with any other clients? | No, we have a dedicated infrastructure |
| What measures are in place to protect the physical security of data centres where our data will be stored? | Data centres are owned and managed by Rackspace |
| Who has access to our data? | Our Customer Services team |
| Is our data on your servers encrypted at rest? | Yes, we use Vormetric encryption to encrypt your SQL data and all your documents |

### Business continuity

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Do you have a business continuity plan that is reviewed, tested and updated at least annually? | Yes |
| When was the business continuity plan last tested? | April 2020 |

### User access

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Who within your organisation will have access to the personal data? | Our Customer Services Team |
| What user authentication do you use on networks/systems that store/process our data? | Our Customer Services team can access your data via a super admin function. This function can only be accessed from the IP address of our offices.  Access to our serves is also tied down to fixed IP addresses and via 2FA. |
| How often are user accounts reviewed for suitability of access levels? | We run a monthly report of who logged in to our severs. |
| What are your password complexity policies? | We have a password policy as part of our ISO 27001 ISMS |

### Penetration / security testing

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Do you conduct penetration testing at least annually on all networks hosting our data | Yes, annually. We have also allow clients to do independent pen tests. |

### Physical security

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Please describe the physical security that protects our data, including building access and physical server access. | Physical security to our servers is managed by Rackspace.  Physical security to our offices is managed by us. |

### Anti-virus

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Do all devices hosting or connecting to our data have AV which is updated at least daily, runs a scheduled scan at least daily, and runs on execution? | Yes, all our laptops use Webroot AV, our servers use Sophos |

### Application development

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Describe the procedures in place to ensure that acceptance criteria for new information systems, upgrades and versions are established and tests are performed prior to roll out. | We have a secure development policy. The development life cycle is the standard Business Requirements 🡪 Functional Specification 🡪 Technical Specification 🡪Development 🡪Units Tests 🡪QA🡪UAT🡪 Live |
| Describe the segregation of duties, including the separation of development, test and operational facilities? | We have separate environments for Development, System Testing, UAT and Live |
| Is production data used in test or development environments? | No |

### Logs

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Do you keep and regularly review access, event, error and transaction logs on all networks storing/processing our data? | Yes, we have Rackspace Managed Security provides active threat detection and remediation for advanced persistence threats (APTs) and other cyber-attacks. |
| Are all logs protected from deletion and/or amendment? | Yes |
| Is access to all logs recorded and monitored? | Yes |

### Breach notification

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Do you have a formal breach notification process | Yes |
| Detail the timelines to notify us of any suspected breach. | We would notify you without delay |
| Have you had a security breach within the last 12 months? If so, please describe the incident, effect and outcome. | No |

### Data retention / deletion

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| For what period do you retain our data? | We never delete your data. How long you retain data on our facility is your responsibility |
| For what period is our data stored in back-ups? | We have a 14 day backup rotation period |
| Where are our backups kept | Slough, UK |

### Data encryption

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Is Personal Data encrypted in transit? Explain how | Yes, using https protocol |
| Is Personal Data encrypted at rest? Explain how | Yes, using Vormetric encryption which encrypts your data and your documents |

### Territories

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Is any our processed, stored or transferred outside of the EEA? | No |

### Sub-processors

|  |  |
| --- | --- |
| **Question** | **Supplier response** |
| Is our data passed on to any third parties for processing? | No |
|  |  |