## Document 7 GDPR Due Diligence Questionnaire. (DPIA Section 3: Supplier Questionnaire)

Instructions for suppliers on completion of the questionnaire;

Suppliers/ Tenderers must ensure they complete each question of this questionnaire, failure to do so may result in rejection of your tender as being non-compliant and your exclusion from the tender process.

*Attachments*

Any attachments you propose to include as part of/ in support of your response must contain the name of your Organisation in the title along with the appropriate question number as indicated and enclosed within square brackets at the beginning of the attached document’s file name e.g. [Tenderer x Q7].

Failure to do so may mean the attachment may not be read and therefore may not be taken into consideration as part of your tender response.

|  |  |
| --- | --- |
| **Company Details** | |
| Company Name: |  |
| Company Address: |  |
| Company Number: |  |

|  |  |
| --- | --- |
| **Contract /Service Details** | |
| Contract Name/Service Description |  |
| Contract Ref |  |

|  |  |  |
| --- | --- | --- |
| 1. **General Data Protection Regulations 2018 (GDPR)** | | |
| Please confirm your that your Organisation complies with the Requirements of GDPR 2018 and Data Protection Act (2018) | | |
| Yes |  |  |
| No |  |  |
|  | | |

|  |  |  |
| --- | --- | --- |
| 1. **Data Protection Breach** | | |
| Has action been taken against your organisation, or a third party involved in your proposed delivery of the contract, by the ICO by in the last 12 months? | | |
| Yes |  |  |
| No |  |  |
|  | | |
| If Yes, please complete the table below:   |  |  |  | | --- | --- | --- | | Date Reported | Breach Detail | Details of action taken | |  |  |  | | | |
|  | | |
| Has your organisation or any other person who has powers of representation, decision or control in the organisation been convicted of breaching GDPR 2018? | | |
| Yes |  |  |
| No |  |  |
| |  |  |  | | --- | --- | --- | | Date Reported | Breach Detail | Details of action taken | |  |  |  | | | |
| 1. **Controller Registration ( PASS/FAIL)** | | |
| As stated in the Specification, the Successful Tenderer(s) **must** be registered as a Controller with the Information Commissioners Office (ICO). This is a mandatory requirement if you are processing Personal Identifiable Data on behalf of Magenta Living, if you are not registered with the ICO as Controller then your tender will be rejected. | | |
| Please confirm your organisation is registered as a Controller with the ICO | | |
| Yes |  |  |
| No |  |  |
|  | | |
| If Yes, please state Notification reference/registration number(s) below. | | |
|  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Data Protection Officer (DPO) Details** | | | |
| Please provide the name and position held within the company of your DPO | | | |
| Name: |  | | |
| Contact details: | |  | |
| Position in company: | | |  |

|  |
| --- |
| 1. **Data Provision** |
| Please confirm which of the data types below are sufficient for you to fulfil the contract.   |  |  |  |  | | --- | --- | --- | --- | | **Data Type** | **Yes/No** | **Data Type** | **Yes/No** | | Name: |  | Trade Union Membership: |  | | Address: |  | Political Opinion: |  | | Date of Birth: |  | Photographs: |  | | Telephone Number: |  | Location Data: |  | | E-Mail Address: |  | Disability Details: |  | | Financial Informtaion: |  | Biometric/ Genetic data: |  | | Medical/ Healthcare Information: |  | Online Identifier |  | | Criminal offences / Convictions: |  | System References |  | | Religious Beliefs: |  | Notepad Details |  | | Other: | | | | |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| 1. **Use of personal data** | | |
| Is it your intention to use the personal data provided by Magenta Living for purposes other than servicing the Contract? | | |
| Yes |  |  |
| No |  |  |
|  | | |
| If Yes, please state below the additional purpose(s) and the type of data (e.g. name, address, contact details etc) | | |
| ***Insert your response below*** | | |
|  | | |

|  |
| --- |
| 1. **Policies, procedures and processes** |
| As a minimum your company **must have** the following policies, procedures and processes in place:   * Information Security Management * GDPR Staff Training and Awareness * Data Retention and Disposal   This is a mandatory requirement.  Please note that you may be required to provide evidence to validate your response |
| From the table below, please state which of the policies, procedures and processes your company has in place. Please indicate Yes or No (Y/N) to each   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Information Governance | Y/N | Information Security Management – Mandatory requirement | Y/N | Business Continuity/Disaster Recovery | Y/N | | GDPR Staff Training and Awareness - Mandatory requirement | Y/N | Data Retention and Disposal - Mandatory requirement | Y/N | Data Breach Incident Management | Y/N | | Data Sharing and Transfer | Y/N | Individual Information Rights (Privacy Policy) | Y/N | Management of Processors and Sub-Processors | Y/N | |

|  |
| --- |
| 1. **Data Management** |
| Under Data Protection the *Contract/Framework Agreement*\* (delete as necessary) specifies the period you are required to retain data.Following this period, you are required to return/delete the information.  Please provide details below of how you propose to manage this requirement. |
| ***Insert your response below*** |
|  |
| 1. **Data Processing** |
| Please provide details of where your organisation will be processing Magenta Living’s Data  Please (**X**) all that apply   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Own Premises |  | Sub - Contractors |  | Cloud Computing |  | Other |  |   If Other (please describe): |

|  |
| --- |
| 1. **Data Flow** |
| Please describe how, or provide a data flow diagram showing how, your process/solution handles Magenta Living’s Data. |
| ***Insert your response below*** |

|  |
| --- |
| 1. **Data Security** |
| Please describe how you will keep the personal data provided to you by Magenta Living secure. |
| ***Insert response below*** |

|  |  |  |
| --- | --- | --- |
| 1. **Data Protection Training** | | |
| Have you conducted data protection training for your employees and other stakeholders whom will be responsible for delivering this Contract? | | |
| Yes |  |  |
| No |  |  |
|  | | |
| If Yes, please state who was trained (i.e. post title, teams) and the most recent date of that training. | | |
| ***Insert your response below*** | | |

|  |  |  |
| --- | --- | --- |
| 1. **Sub-contractors (Sub-processors)** | | |
| Where you propose to sub-contract elements of the Contract, do you have formal contracts in place with your third-parties (sub-processors) that include data protection clauses | | |
| Yes |  |  |
| No |  |  |
| N/A |  |  |
|  | | |
| If Yes, please broadly state the data protection controls you have in place with sub-processors (i.e. who and what systems). If no, please state why. | | |
| ***Insert your response below*** | | |
|  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tender Response completed by** | | | |
| Name: |  | | |
| Role in Organisation: | | |  |
| Signature: | |  | |