# APPENDIX 4

# 

**Data Protection  
Due Diligence Questionnaire**

|  |  |
| --- | --- |
| Version: | 1 |
| Date of version: | 12-01-2023 |
| Created by: | Head of ICT |
| Next review date | 12-03-2024 |
| Approved by: | DPO |
| Confidentiality level: | Public |

**Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Purpose**

This due diligence questionnaire (DDQ) provides evidence of the due diligence carried out by Royal Hospital Chelsea relative to the sharing of personal data under a data sharing agreement, data processing agreement or joint controller arrangement.

The questionnaire should be completed prior to any agreement or contract being signed, and thereafter, periodically during the lifetime of any data sharing arrangement.

The purpose of the questionnaire is to:

1. Assess the technical and organisational measures implemented by a data processor, to ensure the safety, security and legal processing of any personal data entrusted to the data processor. The answers provided will inform the vendor risk assessment (VRA), conducted by the controller, before a data processing contract is signed; or
2. Assess the technical and organisational measures implemented by other controllers, with whom personal data will be shared (either independently or jointly); or,
3. Assess the technical and organisational measures implemented by third parties i.e. organisations that are neither data processors nor independent controllers; and,
4. Conduct periodic checks on independent controllers, data processors or third parties during the lifetime of any data sharing arrangement.

Copies of the initial and periodic questionnaires should be retained by all parties throughout the lifetime of any data sharing arrangement and for at least 6 months thereafter.

**QUESTIONNAIRE**

**Basic Information**

| **ITEM** | **RESPONSE** |
| --- | --- |
| Corporate name |  |
| Other trading name(s) |  |
| Country of incorporation |  |
| Company number |  |
| Registered office address |  |
| Service or project description |  |

**Corporate Governance**

| **ITEM** | **YES/NO** | **COMMENTS** |
| --- | --- | --- |
| Is the organisation registered with the ICO? If so, what is the Registration Number? |  | Registration No: |
| Has the organisation appointed a DPO? If so, please provide relevant contact details? |  |  |
| Is the organisation based outside of the UK/EU? If so, is there a UK or EU representative in place if required and, if so, please provide relevant contact details. |  |  |

**Policies and Procedures**

| **ITEM** | **YES/NO** | **COMMENTS**  **(Title, Version, Date Approved)** |
| --- | --- | --- |
| Does the organisation have a Data Protection Policy? |  |  |
| Does the organisation have an Information Security Policy? |  |  |
| Does the organisation have a Vendor/Third Party Risk Management Policy /Procedure? |  |  |
| Does the organisation have a Physical Security Policy/Procedure? |  |  |
| Does the organisation have a ‘Destruction Policy’ or ‘Electronic Shredding Policy’? |  |  |
| Does the organisation have policies and procedures to facilitate data subject rights e.g. DSAR? |  |  |
| Are staff required to read data protection policies and procedures? If so, how often? |  |  |

**Security**

| **ITEM** | **YES/NO** | **COMMENTS** |
| --- | --- | --- |
| What controls are in place to prevent unauthorised viewing, copying, or emailing of customer information stored in the cloud? |  |  |
| Does the organisation perform regular backups and how fast can the organisation perform a ‘Restore’ if needed? |  |  |
| Does the organisation encrypt all data transmissions, including all server-to-server data transmissions within its own Data Centre(s)? |  |  |
| Does the organisation maintain transaction logs? If so, what type(s) and who has access to the logs? |  |  |
| Does the organisation store personal data on servers located on its own premises? If so, please state the location of servers. |  |  |
| Does the organisation store personal data on servers managed by a third party i.e. a managed service provider (MSP)? If so, please state the location of the third party’s servers? |  |  |
| In the event the hardware/ software fails or becomes unreliable, does the organisation have measures in place to keep data secure and available? |  |  |
| Does the organisation have a Critical Incident Response Plan (CIRP)? |  |  |
| Does the organisation maintain a Business Continuity Plan (BCP)? If so, please state when he BCP was last tested. |  |  |
| Does the BCP include the use of a Disaster Recovery Site (DSR)? If so, when was the ‘failover’ to the DRS last tested. |  |  |
| Is the organisation ISO 27001 certified? If so, what is within the scope of the certification? |  |  |
| Has the organisation achieved Cyber Essentials or Cyber Essentials Plus certification? If so, when? |  |  |
| Are staff required to sign a Confidentiality / Non-Disclosure Agreement (NDA)? |  |  |

**Staff Training**

| **ITEM** | **YES/NO** | **COMMENTS** |
| --- | --- | --- |
| Is data protection training provided to staff? If so, how often? |  |  |
| Is tailored data protection training provided to staff in particular roles? Please provide an overview. |  |  |
| Is information security training provided to staff? If so, please provide details including frequency of training. |  |  |
| Are ‘Knowledge tests’ undertaken on completion of the aforesaid training? If so, are the results centrally recorded? |  |  |

**Personal Data Breaches**

| **ITEM** | **YES/NO** | **COMMENTS** |
| --- | --- | --- |
| Has the organisation had cause to notify any personal data breaches to the ICO or other data protection authority in the past 12 months? |  |  |
| Has regulatory action been taken against the organisation by the ICO or other data protection authority in the past 12 months? |  |  |
| Is the organisation currently subject to regulatory action or ongoing investigation by the ICO or other data protection authority? |  |  |

**Review and Sign-off (For RHC internal use only)**

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/TITLE/date** | **Notes** |
| Reviewed by DPO: |  | *Compliance with data protection legislation e.g., UK GDPR etc.* |
| Comments: | | |
| **Item** | **Name/TITLE/date** | **Notes** |
| Approved by: |  | *Responses to any issues or concerns raised by the DPO should be entered here. Equally, responses to any issues or concerns raised by any of the parties who were consulted about any aspect of this DDQ should be entered here also.* |
| Comments: | | |