**ANNEX B9**

**Personal Data Processing Statement**

**Bidder Guidance:**

This Annex is a Personal Data Processing Statement which should set out the technical and organisational measures the Bidder has in place to comply with the Data Protection Legislation.

Please note that all responses should only describe technical and organisational data protection measures that are relevant to the Services offered in your Tender Response.

This should include as a minimum:

(i) the types of Personal Data which the Bidder and/or its Subcontractors Process or will Process under the Contract;

(ii) the categories of Data Subjects whose Personal Data the Bidder and/or its Subcontractors Process or will Process under the Contract and the nature and purpose of such Processing;

(iii) the locations at which the Bidder and/or its Subcontractors Process or will Process Personal Data under the Contract;

(iv) the Protective Measures that the Bidder and, where applicable, its Subcontractors have implemented to protect Personal Data Processed under the Contract against a Breach of Security (insofar as that Breach of Security relates to data) or a Personal Data Breach;

Locations must include details of all countries where Personal Data will be stored, processed, accessed or managed under the Contract including the locations of data centres, service desks and Network and/or Security Operations Centres. Where any of these locations are outside the European Economic Area (EEA), your response should set out the controls that you will be relying on for storing, processing, accessing or managing Personal Data including Standard Contractual Clauses, Binding Corporate Rules, the country has an Adequacy Decision etc.

Your description of Protective Measures must include details of the technical facilities and measures (including systems and processes) you have in place to ensure compliance with the Data Protection Legislation (including UK – General Data Protection Regulation, the amended Data Protection Act 2018 and the EU GDPR (where applicable)), including effective implementation of the data protection principles and ensuring the protection of the rights of Data Subjects ‘data protection by design and by default’. Your response should include, but should not be limited to facilities and measures:

• to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

• to comply with the rights of Data Subjects in respect of receiving privacy information, and access, rectification, deletion and portability of Personal Data;

• to ensure that any consent-based Processing meets standards of active, informed consent, and that such consents are recorded and auditable;

• to ensure legal safeguards are in place to legitimise transfers of personal data outside the EU (if such transfers will take place);

• to maintain records of Personal Data Processing activities; and

• to regularly test, assess and evaluate the effectiveness of the above measures.

For the avoidance of doubt, the reference to Subcontractors for the purposes of the statement includes the supply chain for the delivery of the Contract, whether those suppliers be direct or indirect. The description of Protective Measures must include details of the due diligence carried out on such third parties to ensure that they are capable of providing the level of protection for the Personal Data as is required by the Contract; and details of the agreements in place with such third parties as required under applicable Data Protection Legislation.

Where applicable to the Services offered in your Tender Response, you must also set out whether there are any categories of Personal Data where the Supplier will be the Controller and the Authority the Processor and/or the Parties will be Joint Controllers under the Contract. Where this is the case, your response should clearly set out the scope of applicable Personal Data.

**Bidder Response (1,500 words maximum):**

**This is a PASS/FAIL section.**  
  
Providing a satisfactory response will result in your response receiving a PASS for this question. Providing an unsatisfactory response will result in your response receiving a FAIL for this section. This will result in your response being rejected and you will not be invited to participate further in this procurement.  
  
The response will not be scored but instead will be evaluated based on a risk based approach in which the Trust will assess the risk exposure based on the ability of the Supplier's response to ensure compliance with Data Protection Legislation and ensure the protection of the rights of data subjects.  
  
This evaluation will be conducted on the following basis:  
  
Full Satisfactory Response with no areas of concern (Low Risk)  
Partially Satisfactory Response with some cause for concern (Medium Risk)  
Unsatisfactory Response  with significant cause for concern (High Risk)  
No Response - Non-Compliant  
  
If a Bidder provides no response or an unsatisfactory response then they will receive a FAIL for this question.

Bidders should note that in assessing the level of risk, the Trust will assess whether the technical and organisational measures in place in relation to data protection are sufficient to ensure that the services comply with Data Protection Legislation including the Data Protection Act 2018 and UK GDPR.

**ANNEX B2b**

**Information Governance Due Diligence Questionnaire**



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Information Governance Compliance Programme** | | | |  |
|  |  |  |  | |  |
| **No** | **Question** | **Answer** | | |  |
| 1 | **Name of organisation** |  | | |  |
| If a subsidiary company, please enter the name of the parent company |  | | |  |
| Does the parent company have the power to hold the subsidiary company to account for its performance? |  | | |  |
| Company / Charity Number |  | | |  |
| Registered Address |  | | |  |
| Number of Employees |  | | |  |
| 2 | **Name of main contact** |  | | |  |
| Contact Job title |  | | |  |
| Contact Email |  | | |  |
| Contact Telephone |  | | |  |
| 3 | **Data Protection Notification Number** If you are exempt from having to register with the ICO please explain the reasons why. Please also include registration with other Supervisory Authority as relevant |  | | |  |
| 4 | **Department of Health’s Data Security and Protection Toolkit Registration and Score** Formerly known as IG Toolkit submission |  | | |  |
| 5 | **Organisation compliance with the Data Protection Legislation** |  |  | |  |
| 6 | **Business insurances**  e.g. professional indemnity, employer's liability, public/product liability. |  |  | |  |
| 7 | **ISO 27001 / ISO 27002** | | |  | | |  |
| 8 | **Cyber Essentials** | | |  | | |  |
| 9 | **Do you have any of these:** | | | **Yes/No** | | **Further info** |  |
| ISO 9001 (Quality management system) | | |  | |  |  |
| ISO 20000 (IT service management | | | Yes | |  |  |
| ISO 22301 (Business continuity management) | | |  | |  |  |
| ISO 29100 (Privacy framework standard) | | |  | |  |  |
| ISO 27017 (Cloud specific controls) | | |  | |  |  |
| ISO 27018 (Personal data protection) | | |  | |  |  |
| ISO 27701 (Privacy information management system) | | |  | |  |  |
| PCI DSS | | |  | |  |  |
| G-Cloud Framework | | |  | |  |  |
| Cloud Computing Standards | | |  | |  |  |
| SOC Report | | |  | |  |  |
| Transaction Monitoring | | |  | |  |  |
| Any other compliance programme you have that is not listed here, please list them in the next column | | |  | | |  |
|  | | |  |
|  | | |  |
| 10 | **Data protection or cyber security breach** within the last 3 years requiring external reporting  i.e. to ICO, European Supervisory Authority, NCSC | | |  | |  |  |
| 11 | **International data transfers scheme** Do you have appropriate safeguards to make a restricted transfer of personal data outside of the UK/EEA, i.e. standard contractual clause, Privacy shields, Binding Corporate Rules, etc. | | |  | |  |  |
| 12 | **Additional info/comments** | | |  | | |  |
|  |  | | |  | |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Information Security Self-Assessment** | |  |  |  |  |  |  |
| Third parties working with the Trust that does not hold ISO 27001 certification must complete these questions. | |  |  |  |  |  |  |
| **Data Protection Overview** | | **Answer** | | | | **IG Notes** |  |
| **Storage** | | | | | | |  |
| 1 | Will you process Trust information outside the EU? (*Please refer to the definition of "processing" under the Guidance tab.)* | *If YES, please provide details on where* | | | |  |  |
| 2 | Is/would the information you process on behalf of the Trust be held at the company address you have provided? | *If YES then please provide the address of the other site(s) in Q3* | | | |  |  |
| 3 | If the answer to Question 2 is NO, please provide details of all the addresses where the information will be processed (e.g. stored). |  | | | |  |  |
| 4 | Please indicate the minimum types of personal information you will be processing in order to provide this Service.  *Enter Yes/ No/ Not Known next to each data item or delete items you won't process  Any not listed state under 'Other'* | Name |  | Religion |  |  |  |
| Address |  | Ethnicity |  |  |  |
| Post code (no of digits |  | Sexual orientation |  |  |  |
| NHS No |  | Diagnosis |  |  |  |
| Local identifiers |  | Medical history |  |  |  |
| NI Number |  | Date of birth |  |  |  |
| Gender |  | Occupation |  |  |  |
| IP address |  | Biometric data |  |  |  |
| 5 | Other *(Please detail):* |  | | | |  |  |
| 6 | If collecting personal information from individuals on behalf of the Trust do/will you explain to the individuals the reasons as to why you are gathering the information, the exact purposes for which it will be used and any other parties who it may be shared with? | If YES, please provide details on how you do this including your Privacy Information: If you do not collect information on the Trust’s behalf please state ‘Not Applicable’: | | | |  |  |
| 7 | If collecting personal information from individuals on behalf of the Trust do/will you provide a copy of the Trust's Privacy Policy? |  | | | |  |  |
| 8 | With regard to the personal information you process on behalf of the Trust – do/will you disclose this information to anyone other than the Trust? | If the answer is YES, please provide examples and reasons: | | | |  |  |
| 9 | Would Trust Data be encrypted while at rest (i.e. data stored on servers, desktops and laptops)? |  | | | |  |  |
| 10 | Would Trust Data be segregated from that of your organisation and other clients? |  | | | |  |  |
| **Physical Security** | | | | | | |  |
| 11 | If you have a publically accessible reception area how is it controlled? |  | | | |  |  |
| 12 | If there are any other entrances or exits, how are these controlled? |  | | | |  |  |
| 13 | Is the office area, where personal data is viewed, visible from reception or from outside? | *If NO please go to question 16* | | | |  |  |
| 14 | What measures do you have in place to mitigate the risk of screens/information being overlooked e.g. Screen filters, frosted glass, blinds? |  | | | |  |  |
| 15 | Do you have a clear desk policy in place whereby all material, regardless of protective marking, are to be removed from the user’s desk at the end of the day and stored in an appropriate lockable container for the type of material held? | *If yes when was it last reviewed and updated?* | | | |  |  |
| 16 | Do you have a lock screen policy? | *If NO please go to question 19. If yes when was it last reviewed and updated?* | | | |  |  |
| 17 | Do screens automatically lock if the station has been inactive for a period of time? If yes please provide the time limit. |  | | | |  |  |
| 18 | Is all confidential information locked securely when not in use? |  | | | |  |  |
| 19 | Are all data bearing electronic devices securely locked away when not in use? |  | | | |  |  |
| 20 | Do you have a key management procedure in place? |  | | | |  |  |
| 21 | Do Staff wear a name badge or similar whereby they can be identified as belonging to your organisation? |  | | | |  |  |
| 22 | Do you have a visitors/contractor signing in and out process? |  | | | |  |  |
| 23 | Are visitors/contractors required to wear a badge or similar for identification purposes? |  | | | |  |  |
| 24 | Are there any other measures taken to ensure that access to the premises is restricted to authorised staff and visitors only? | *If YES then please provide details* | | | |  |  |
| 25 | Do you have an electronic card access system whereby access to your premises by your staff and visitors is logged and the data is auditable? |  | | | |  |  |
| 26 | Do you have a Policy/Procedure in place for disabling lost/stolen access cards and collecting cards from leavers? | *If yes when was it last reviewed and updated?* | | | |  |  |
| 27 | Are there fire and intruder alarm systems protecting the premised? | *If NO then please go to question 30* | | | |  |  |
| 28 | Is the alarm system linked to the fire service/police/security service? |  | | | |  |  |
| 29 | Are windows secure? E.g. locked, blinds etc… |  | | | |  |  |
| 30 | Are the premises where the information is kept protected by CCTV, security patrols etc. |  | | | |  |  |
| 31 | Are restricted areas of the office accessible to only those with authorised to access them? |  | | | |  |  |
| 32 | What arrangements do you have in place for the secure disposal of confidential paper waste? | *Please provide details of the company used* | | | |  |  |
| 33 | Are your Servers/Comms Cabinet based in an access controlled room? | *If NO please give details of where they stored and what security controls are in place.* | | | |  |  |
| 34 | Are access rights to this room reviewed regularly? |  | | | |  |  |
| 35 | Is this room of solid construction to prevent unauthorised access? |  | | | |  |  |
| 36 | If this room is shared, are the servers/comms equipment kept in locked cabinets? |  | | | |  |  |
| 37 | Are your staff prohibited from using the server/comms room as a storage area? |  | | | |  |  |
| 38 | Are the servers/comms equipment protected by a UPS? |  | | | |  |  |
| 39 | Does the room in which Servers/Comms equipment are located have both, fire and intruder detection? |  | | | |  |  |
| 40 | Is air conditioning installed in the room servers/comms cabinets are housed? |  | | | |  |  |
| 41 | Do you carry out regualr internal information security audits? |  | | | |  |  |
| **People and Policy** | | | | | | |  |
| 42 | What measures are in place to ensure that all staff are aware of their legal responsibilities under the Data Protection Legislation? | *E.g. training, employment checks/ conditions, communications plans* | | | |  |  |
| 43 | How often is information security training provided? |  | | | |  |  |
| 44 | Are records maintained of any information security/data protection related training received by your staff? |  | | | |  |  |
| 45 | Does your training include what staff should do in the event of a personal data breach? |  | | | |  |  |
| 46 | Are all staff vetted to BPSS standards? |  | | | |  |  |
| 47 | Are DBS checks carried out on staff? If so at what interval are these renewed? If only selected staff are DBS checked, please advise of the criteria for this. |  | | | |  |  |
| 48 | Does a confidentiality statement/clause form part of your employment contracts? |  | | | |  |  |
| 49 | Can it be demonstrated that a breach of the policies is a disciplinary offencewithin your organisation? | *If YES, please provide details on how you do this* | | | |  |  |
| 50 | Do you have a leavers Policy and Procedure which ensures that leavers accounts are disabled on leaving employment and any access cards returned/disabled? |  | | | |  |  |
| 51 | What policy, procedures, training or other measures have you taken to adopt the security standard ISO27001/2? | *Please provide details, including if applicable why you have not adopted the standard.* | | | |  |  |
| 52 | Do you have an approved Data Protection and/or Information Security Policy in place? | *If yes when was it last reviewed and updated? Is it available to all staff/relevant thrid parties?* | | | |  |  |
| 53 | Do you have an Acceptable use of I.T. Policy in place that covers the use of e-mail and the internet? | *If yes when was it last reviewed and updated?* | | | |  |  |
| 54 | How do you monitor compliance with these policies? |  | | | |  |  |
| 55 | Do you control what websites your employees are able to access e.g. by white listing? |  | | | |  |  |
| 56 | Do you use an e-mail Spam Filter? |  | | | |  |  |
| **Remote Working and Portable Devices** | | | | | | |  |
| 58 | Will any of your staff processing Trust information work remotely? |  | | | |  |  |
| 59 | Do you have a remote working policy? | *If yes when was it last reviewed and updated?* | | | |  |  |
| 60 | Does this include requirements for transporting data e.g. not to leave unattended or locked in a car overnight? |  | | | |  |  |
| 61 | Are laptops secured using full hard disk encryption with a minimum FIPS 140-2 compliant standard software. |  | | | |  |  |
| 62 | Are mobile devices, such as Blackberry, Android, Apple or Windows be secured using the appropriate encryption service for that device to a minimum level of AES 256? |  | | | |  |  |
| 63 | Are all electronic sensitive information residing on your ICT network which are accessed remotely secured as per commercial best practice set out in ISO/IEC 27033-4 audited/accredited annually? | *If YES please provide a copy of you certificate* | | | |  |  |
| 64 | How is remote access authenticated? |  | | | |  |  |
| 65 | Do you restrict staff from connecting portable devices such as USB memory sticks to their work computers? | *If YES, please provide details on how you do this* | | | |  |  |
| 66 | In cases where removable media is used, will only devices with FIPS 140-2 standard software e.g. Kingston DataTraveller 4000 be used? |  | | | |  |  |
| 67 | Are staff provided with a means to secure their laptop e.g. a Kensington Lock? |  | | | |  |  |
| **Sub Contractors** | | | | | | |  |
| 68 | Will you use third parties (e.g. Sub- Contractors) to process any of the Trust’s information as part of this contract. | *If NO then please go to question 74* | | | |  |  |
| 69 | Please provide the names and addresses of the companies you will be using as subcontractors for this contract. |  | | | |  |  |
| 70 | How do you ensure that the sub-contractors you use have sufficient technical and organisational safeguards in place to protect Trust Data you might have to share with them? |  | | | |  |  |
| 71 | Please provide details of the measures you have in place to ensure their staff are vetted to a minimum of the Baseline Personnel Security Standard (BPSS). |  | | | |  |  |
| 72 | Please provide details of the ongoing training they provide to staff in respect of data security, including the identification and reporting of security incidents. |  | | | |  |  |
| 73 | Please describe their disciplinary procedures in the event of a security breach involving Lead/Customer Organisations Data. |  | | | |  |  |
| **Transfer of data** | | | | | | |  |
| 74 | Is data encrypted in transit / accessed using secure protocols (e.g. sFTP, SSH, TLS etc) when communicating with untrusted networks? |  | | | |  |  |
| 75 | Depending upon the nature of the contract, the information shared with you may or may not be highly confidential.   Where the Trust classifies information as 'confidential' it must be delivered and received by secure means, e.g. secure connection (HTTPS).  Please describe below the facilities/options you have at your disposal to provide for the safe receipt and delivery of confidential information. |  | | | |  |  |
| 76 | Do you have access to automated electronic secure transmission via the Government Secure Internet (GSI) with the appropriate level of security control? |  | | | |  |  |
| 77 | Where sensitive information is attached and sent via email will it first be compressed and encrypted using Zip strong encryption (AES 256) from end to end (i.e. nhs.net to nhs.net) or deploying a DLP tool? |  | | | |  |  |
| 78 | The use of removable media should be avoided where possible.  If the use of removable media is approved by us, will your staff understand that the Trust data transfer must be carried out in a secure, centralised environment? |  | | | |  |  |
| 79 | Where sensitive information is transferred to CD-ROM removable media, will it first be compressed and encrypted using zip strong encryption (AES 256)? |  | | | |  |  |
| 80 | When sending sensitive Trust Data via post, it must be sent by Special Delivery (with track and trace facility) in a double envelope and issued with a transmittal. The outer envelope must not show any marking or descriptor other than 'Personal' or details of the addressee only. The inner envelope must be marked with the appropriate protective marking and be suitably addressed. Do your staff comply with these requirements? |  | | | |  |  |
| 81 | Confidential Trust Data may only be sent by fax within the UK and following written authorisation by the Trust IG department. Staff must ensure that the recipient is able to receive the fax immediately and confirm that they have the correct number. Do your staff comply with these requirements? **The transmittal fax machine must issue a transmittal receipt. Anything marked OFFICIAL-SENSITIVE must never be faxed.** |  | | | |  |  |
| **Disposal of hardware/software** | | | | | | |  |
| 82 | How do you safely and securely dispose of obsolete hardware and software from which information could be recovered. | *Please provide details of the company used.* | | | |  |  |
| **Data records** | | | | | | |  |
| 83 | Do you have the facility to identify and delete all records relating to a specific Data Subject (both physical and electronic) if required? |  | | | |  |  |
| 84 | Will your staff be made aware of how to respond to a Data Subject Access Request involving Trust Data? i.e. that the request would be dealt with by the Trust and we would need to be notified immediately on receipt of the request? |  | | | |  |  |
| 85 | Do you ensure your staff are aware that any Data Subject requests for Trust Data must be directed to the Trust without any undue delay? |  | | | |  |  |
| **Business Continuity and Disaster Recovery Plan** | | | | | | |  |
| 86 | Are you certified to the ISO 23001 standard? |  | | | |  |  |
| 87 | Do you have a Formal Disaster Recovery/Business Continuity Plan in place? | *If YES when was it last reviewed and updated? If NO please go to question 94* | | | |  |  |
| 88 | At what intervals are your Business Continuity plans tested? |  | | | |  |  |
| 89 | When was it last tested? |  | | | |  |  |
| 90 | What were the results of this test? |  | | | |  |  |
| 91 | Are individuals aware of their roles and responsibility in the event that a Business Continuity Plan is invoked? |  | | | |  |  |
| 92 | Is documentation maintained on incidents / events (issues, notifications, outcomes, and remediation)? |  | | | |  |  |
| 93 | Is post incident analysis carried out in order to identify 'lessons learned'? |  | | | |  |  |
| 94 | Please provide details of how you would ensure continuity of service to The Trust in the event of a serious incident/disaster. |  | | | |  |  |
| **Incident handling** | | | | | | |  |
| 95 | Have you had a security breach resulting in loss or damage to personal or confidential data or unauthorised disclosure of personal information in the last 2 years? | *If YES then please provide details* | | | |  |  |
| 96 | Have you been subject to any complaints to the ICO in the last 2 years? | *If YES then please provide details including the outcome of the complaint(s)* | | | |  |  |
| 97 | If yes to question 95 or 96 did this involve information which you were processing on behalf of a Data Controller? |  | | | |  |  |
| 98 | Do you have a Data Protection Officer? If yes please provide their contact details? |  | | | |  |  |
| 99 | Do you have a security incident policy, procedure and standard report form? |  | | | |  |  |
| 100 | Is this communicated and available to all staff? |  | | | |  |  |
| 101 | Are all staff informed about how to report a Personal Data Breach? |  | | | |  |  |
| 102 | Do you keep a record of all Security Events/Incidents. |  | | | |  |  |
| 103 | If a potential/actual Security Event/Incident affecting Trust Data Occurs who will be responsible for reporting this to us, are they aware that we require immediate notification? |  | | | |  |  |
| 104 | Are you aware of the Breach Notification requirements as set out by Data Protection Regulation and the ICO? |  | | | |  |  |
| **System Backups** | | | | | | |  |
| 105 | Do you take backups of the data you process on behalf of the Trust? |  | | | |  |  |
| 106 | At what interval are backups taken? |  | | | |  |  |
| 107 | What is the retention period for backups? |  | | | |  |  |
| 108 | Where are your backups stored? E.G. off site or in a fire proof safe? |  | | | |  |  |
| 109 | Is backup data protected to the same level as production data? |  | | | |  |  |
| 110 | Are backups encrypted? |  | | | |  |  |
| 111 | At what interval do you carry out backup restore tests? |  | | | |  |  |
| **Exit arrangements** | | | | | | |  |
| 112 | All Lead/Customer Organisation Data held electronically (including back-ups) or in hard copy form by the Contractor, must either be returned or destroyed at the end of the project or when access to that data is no longer required, whichever is earliest. When equipment that holds or has held data is disposed of or destroyed, all data must be rendered unreadable and irretrievable. Please set out how you will meet these requirements (covered by DPA) |  | | | |  |  |
| 113 | Where information disposal, of Trust sensitive information, is required, what disposal methods specific to the requirements of the protective marking will you use? |  | | | |  |  |
| **Insurance** | | | | | | |  |
| 114 | Do you have all insurances for your business required by law (e.g. professional indemnity, employer's liability, public/product liability)? |  | | | |  |  |
| 115 | What are the maximum levels of indemnity of the insurance policies you have listed above? |  | | | |  |  |
| 116 | Please provide a copy of all your insurance policies. |  | | | |  |  |
|  |  |  |  |  |  |  |  |