****

**COVER NOTES**

This Protocol updates and replaces the data protection protocol which was published in January 2018 as part of the January 2018 update to the standard NHS Terms and Conditions for the supply of goods and the provision of services. This update reflects changes to the model clauses relating to data protection brought in by the PPN 02/18 which was published in May 2018. Please see the relevant Crown Commercial Service Procurement Policy Notice (**PPN**) and related model clauses (Changes to Data Protection Legislation & General Data Protection Regulation) here:

<https://www.gov.uk/government/publications/procurement-policy-note-0218-changes-to-data-protection-legislation-general-data-protection-regulation>).

As part of this update, the Department of Health and Social Care’s policy approach has been to adopt the Crown Commercial Service PPN model clauses with some changes:

1. to ensure consistent use of terminology with the NHS Terms and Conditions;

2. to add clarity to the scope of the obligations under the PPN in an NHS context; and

3. to allow for appropriate variations. .

This Protocol contains model clauses for completion in connection with relevant contracts where the Supplier will be Processing personal data under or in connection with the Contract, where the parties will be acting as Joint Controllers, or where the parties may be sharing personal data as independent Controllers. This is required by Schedule 3 (Information and Data Provisions) of the NHS Terms and Conditions.

It is important that the Protocol is completed and/or tailored in such a way to reflect the actual data Processing activities taking place under a particular contract. In the context of more complex data sharing arrangement the Protocol will need more substantial changes and tailoring to reflect any data controlled by the Supplier and Processed by the Authority and/or any data shared with third parties as part of such arrangements.

Thought also needs to be given as to whether any changes need to be made to reflect any practical considerations that may apply to a particular contract. For example, the Protocol provides that the Supplier must ensure that it does not transfer Personal Data outside of the EU without the prior written consent of the Authority. If it is impractical for the Authority to provide such consent each and every time an item of Personal Data is transferred, you will need to agree specific overarching provisions with the Supplier as to how to deal with, and manage, such transfers in compliance with Data Protection Legislation.

*Developed in partnership with* 

**September 2019**

**DATA PROTECTION PROTOCOL**

*Guidance: This Data Protection Protocol is for use alongside the NHS terms and conditions. The table at the beginning of the Protocol should be completed by the Authority setting out the nature of the relationship and processing that will be taking place under the Contract.*

**Table A – Processing, Personal Data and Data Subjects**

This Table shall be completed by the Authority, who may take account of the view of the Supplier, however the final decision as to the content of this Table shall be with the Authority at its absolute discretion.

1. The contact details of the Authority’s Data Protection Officer are: **[Insert Contact details**]

2. The contact details of the Supplier’s Data Protection Officer are: **[Insert Contact details**]

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of the Controller and Processor | *[The Parties acknowledge that the Authority is the Controller and the Supplier is the Processor for the purposes of the Data Protection Legislation in respect of:*  *[Insert the scope of Personal Data which the purposes and*  *means of the Processing is determined by the both Parties]*  *In respect of Personal Data where the Authority is the Controller and the Supplier is the Processor, Clause 1 of this Protocol will apply.]*  *[The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:*  *[Insert the scope of Personal Data which the purposes and*  *means of the Processing is determined jointly by the both Parties]*  *In respect of Personal Data under joint control, Clause 2 of this Protocol will apply].*  *[The Parties acknowledge that they are independent Controllers for the purposes of the Data Protection Legislation in respect of:*  *[Insert the scope of Personal Data shared which the purposes and means of the Processing means that they are independent Controllers.]*  *In respect of Personal Data shared under the Contract in circumstances where the Authority and the Supplier are independent Controllers, Clause 3 of this Protocol will apply.]* |
| Subject matter of the  Processing | *[This should be a high level, short description of what the*  *Processing is about i.e. its subject matter of the contract.*  *Example: The Processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public. ]* |
| Duration of the  Processing | *[Clearly set out the duration of the Processing including dates]* |
| Nature and purposes of  the Processing | *[Please be as specific as possible, but make sure that you cover all intended purposes.*  *The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.*  *The purpose might include: employment Processing, statutory obligation, recruitment assessment etc]* |
| Type of Personal Data being Processed | *[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]* |
| Categories of Data  Subject | *[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]* |
| Plan for return and destruction of the data once the Processing is complete  UNLESS requirement under union or member state law to preserve that type of data | *[Describe how long the data will be retained for, how it be returned or destroyed]* |

**Definitions**

The definitions and interpretative provisions at Schedule 4 (Definitions and Interpretations) of the Contract shall also apply to this Protocol. For example, the following terms are defined in Schedule 4 of the Contract: “Authority”, “Controller”, “Process” and “Processer” and “Supplier” are defined in Schedule 4 of the Contract. Additionally, in this Protocol the following words shall have the following meanings unless the context requires otherwise:

|  |  |
| --- | --- |
| “**Data Loss Event**” | means any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach; |
| “**Data Protection Legislation**” | means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of personal data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy; |
| “**Data Protection Impact Assessment**” | means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data; |
| “**Data Protection Officer**” | shall have the same meaning as set out in the GDPR; |
| “**Data Recipient**” | means that Controller who receives the relevant Personal Data; |
| “**Data Subject**” | shall have the same meaning as set out in the GDPR; |
| “**Data Subject Request**” | means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data; |
| “**Data Transferor**” | means that Controller who transfers the relevant Personal Data; |
| “**DPA 2018**” | means the Data Protection Act 2018; |
| “**Joint Controllers**” | means where two or more Controllers jointly determine the purposes and means of Processing; |
| “**LED**” | means the Law Enforcement Directive *(Directive (EU) 2016/680)*; |
| “**Personal Data Breach**” | shall have the same meaning as set out in the GDPR; |
| “**Protective Measures**” | means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, putting in place appropriate training of staff involved in the processing of Personal Data and regularly assessing and evaluating the effectiveness of the such measures adopted by it [including those outlined in Schedule [*insert schedule number and name (e.g. if there is a relevant security schedule*)]]; |
| “**Protocol**” or “**Data Protection Protocol**” | means this Data Protection Protocol; |
| “**Sub-processor**” | means any third Party appointed to Process Personal Data on behalf of that Processor related to this Contract. |

1. SUPPLIER AS DATA PROCESSOR
   1. Where, in Table A, the Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor for the relevant purposes specified in Table A this Clause 1 shall apply. The only Processing that the Supplier is authorised to do is listed in Table A of this Protocol by the Authority and may not be determined by the Supplier.
   2. The Supplier shall notify the Authority immediately if it considers that any of the Authority’s instructions infringe the Data Protection Legislation.
   3. The Supplier shall provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Authority, include:
      1. a systematic description of the envisaged Processing operations and the purpose of the Processing;
      2. an assessment of the necessity and proportionality of the Processing operations in relation to the Services;
      3. an assessment of the risks to the rights and freedoms of Data Subjects; and
      4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
   4. The Supplier shall, in relation to any Personal Data Processed in connection with its obligations under this Contract:
      1. Process that Personal Data only in accordance with Table A, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Authority before Processing the Personal Data unless prohibited by Law;
      2. ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Authority may reasonably reject (but failure to reject shall not amount to approval by the Authority of the adequacy of the Protective Measures), having taken account of the:
         1. nature of the data to be protected;
         2. harm that might result from a Data Loss Event;
         3. state of technological development; and
         4. cost of implementing any measures;
      3. ensure that :
         1. the Supplier Personnel do not Process Personal Data except in accordance with this Contract (and in particular Table A);
         2. it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:
            1. are aware of and comply with the Supplier’s duties under this Protocol;
            2. are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;
            3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Authority or as otherwise permitted by this Contract; and
            4. have undergone adequate training in the use, care, protection and handling of Personal Data;
      4. not transfer Personal Data outside of the EU unless the prior written consent of the Authority has been obtained and the following conditions are fulfilled:
         1. the Authority or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Authority;
         2. the Data Subject has enforceable rights and effective legal remedies;
         3. the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Authority in meeting its obligations); and
         4. the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the Processing of the Personal Data; and
      5. at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination of the Contract unless the Supplier is required by Law to retain the Personal Data.
   5. Subject to Clause 1.6 of this Protocol, the Supplier shall notify the Authority immediately if in relation to any Personal Data Processed in connection with its obligations under this Contract it:
      1. receives a Data Subject Request (or purported Data Subject Request);
      2. receives a request to rectify, block or erase any Personal Data;
      3. receives any other request, complaint or communication relating to either Party’s obligations under the Data Protection Legislation;
      4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Contract;
      5. receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
      6. becomes aware of a Data Loss Event.
   6. The Supplier’s obligation to notify under Clause 1.5 of this Protocol shall include the provision of further information to the Authority in phases, as details become available.
   7. Taking into account the nature of the Processing, the Supplier shall provide the Authority with full assistance in relation to either Party’s obligations under Data Protection Legislation in relation to any Personal Data Processed in connection with its obligations under this Contract and any complaint, communication or request made under Clause 1.5 of this Protocol (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:
      1. the Authority with full details and copies of the complaint, communication or request;
      2. such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
      3. the Authority, at its request, with any Personal Data it holds in connection with its obligations under this Contract in relation to a Data Subject;
      4. assistance as requested by the Authority following any Data Loss Event;
      5. assistance as requested by the Authority with respect to any request from the Information Commissioner’s Office, or any consultation by the Authority with the Information Commissioner’s Office.
   8. The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Protocol. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:
      1. the Authority determines that the Processing is not occasional;
      2. the Authority determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
      3. the Authority determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
   9. The Supplier shall allow for audits of its data Processing activity by the Authority or the Authority’s designated auditor in relation to any Personal Data Processed in connection with its obligations under this Contract.
   10. Each Party shall designate its own Data Protection Officer if required by the Data Protection Legislation.
   11. Before allowing any Sub-processor to Process any Personal Data related to this Contract, the Supplier must:
       1. notify the Authority in writing of the intended Sub-processor and Processing;
       2. obtain the written consent of the Authority;
       3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this Protocol such that they apply to the Sub-processor; and
       4. provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.
   12. The Supplier shall remain fully liable for all acts or omissions of any of its Sub-processors.
   13. The Authority may, at any time on not less than 30 Working Days’ notice, revise this Protocol by replacing it with any applicable controller to Processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).
   14. The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Authority may on not less than 30 Working Days’ notice to the Supplier amend this Protocol to ensure that it complies with any guidance issued by the Information Commissioner’s Office.
   15. The Supplier shall comply with any further instructions with respect to Processing issued by the Authority by written notice. Any such further written instructions shall be deemed to be incorporated into Table A from the date at which such notice is treated as having been received by the Supplier in accordance with Clause 27.2 of Schedule 2 of the Contract.
2. PARTIES AS JOINT CONTROLLERS
   1. Where in, Table A, the Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority and the Supplier are Joint Controllers this Clause 2 shall apply. The only Processing that a Joint Controller is authorised to do is listed in Table A of this Protocol by the Authority and may not be determined by the Supplier.
   2. The Parties shall in accordance with GDPR Article 26 enter into a Joint Controller Agreement based on the terms outlined in Schedule 1.
3. BOTH DATA CONTROLLERS
   1. To the extent that the nature of the Services means that the Parties are acting both as Controllers (as may be referred to in Table A), each Party undertakes to comply at all times with its obligations under the Data Protection Legislation and shall:
      1. implement such measures and perform its obligations (as applicable) in compliance with the Data Protection Legislation;
      2. be responsible for determining its data security obligations taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects, and implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful Processing and accidental destruction or loss and ensure the protection of the rights of the Data Subject, in such a manner that Processing will meet the requirements of the Data Protection Legislation where Personal Data has been transmitted by it, or while the Personal Data is in its possession or control;
      3. where appropriate, promptly refer to the other Party any requests, from (i) Data Subjects in regards to the right of access to Personal Data by that Data Subject in accordance with the Data Protection Legislation; (ii) the Information Commissioner; or (iii) any other law enforcement authority and to the extent it is reasonable and practical to do so consult with the other Party (for the avoidance of doubt at no additional cost) before responding to such request.
   2. Where Personal Data is shared between the Parties, each acting as Controller:
      1. the Data Transferor warrants and undertakes to the Data Recipient that such Personal Data have been collected, Processed and transferred in accordance with the Data Protection Legislation and this Clause 3;
      2. the Data Recipient will Process the Personal Data in accordance with the Data Protection Legislation and this Clause 3; and
      3. where the Data Recipient is in breach of its obligations under this Protocol and the Data Protection Legislation, the Data Transferor may temporarily suspend the transfer of the Personal Data to the Data Recipient until the breach is repaired.

*Guidance: there are limited requirements in the GDPR when parties act as separate Controllers. Clause 3 above provides a sensible starting point. However, Authorities are advised to review the Information Commissioner’s Guidance (*[*ICO GDPR Guidance*](file:///C:\Users\NJAW\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\4NUXDV4E\ICO%20GDPR%20Guidance)*) and consultant their Information Governance team when considering whether further provisions or a separate data sharing agreement should be used.*

1. CHANGES TO THIS PROTOCOL
   1. Subject to Clauses 1.13, 1.14 and 1.15 of this Protocol, any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.

**Schedule 1 – Joint Controller Agreement**

In this Schedule the Parties must outline each party’s responsibilities for:

 providing information to data subjects under Article 13 and 14 of the GDPR.

 responding to data subject requests under Articles 15-22 of the GDPR

 notifying the Information Commissioner (and data subjects) where necessary about data breaches

 maintaining records of Processing under Article 30 of the GDPR

 carrying out any required Data Protection Impact Assessment

The joint controller agreement must include a statement as to who is the point of contact for data subjects. The essence of this relationship shall be published. You may wish to incorporate some clauses equivalent to those specified in Clause 1.2-1.14 of Clause 1.

Situations where both parties act as Joint Controllers are likely to be relatively novel. Therefore, in such circumstances, it will be important to seek specific legal advice on the approach to the joint controller agreement. As part of this, you may wish to include an additional clause apportioning liability between the parties arising out of data protection in respect of data that is jointly controlled.