

Where the Parties are Joint Controllers of Personal Data


16. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement Paragraphs that are necessary to comply with GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

Independent Controllers of Personal Data

17. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
18. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
19. Where a Party has provided Personal Data to the other Party in accordance with Paragraph 7 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
20. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
21. The Parties shall only provide Personal Data to each other:
- (a) to the extent necessary to perform their respective obligations under the Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and
 - (c) where it has recorded it in Annex 1 (Processing Personal Data).
22. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.
23. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30

GDPR and shall make the record available to the other Party upon reasonable request.

24. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):
- (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
25. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
- (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
26. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
27. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).



Joint Schedule 11 (Processing Data)

Crown Copyright 2019

28. Notwithstanding the general application of Paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data Template

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

- 1.1 The contact details of the Relevant Authority's Data Protection Officer are: [REDACTED] (interim) email: nhsdigital.dpo@nhs.net
- 1.2 The contact details of the Supplier's Data Protection Officer are: **gdpr@netcompany.com**
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

For the avoidance of doubt, access to personal data is not expected to be generally necessary for the scope of the Services outlined in the Statement of Requirements for C30669 and the Order Form, and the Supplier Personnel shall not generally have access to any personal data of NHS Digital. However, it is recognised that on occasion it may become necessary for NHS Digital to require services associated, where the Supplier will be given access to personal data. Where any such service request gives access to personal data, the Supplier shall access such data as processor to NHS Digital, and the following table shall apply (as updated where necessary in the agreed Statements of Work).

Description	Details
Identity of Controller for each Category of Personal Data	<p>NHS Digital is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with Paragraph 2 to Paragraph 15 and for the purposes of the Data Protection Legislation, NHS Digital is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p><i>Any information accessed on NHS Digital systems as part of the Services, including:</i></p> <ul style="list-style-type: none">• <i>Patient / citizen : demographics data: NHS number, name, address, postcode, language preferences and contact information relation to subjects.</i>• <i>Patient / citizen: clinical data: NHS number, details of subject's health, historic information regarding subject's health.</i>• <i>NHS Digital staff information</i>• <i>Wider NHS staff information</i>

	<p>Further details of the information assets hosted on the listed platforms are detailed in the NHS Digital Unified Registry. To note, NHS Digital may solely be a processor to another government controller, and in which case the Supplier shall remain NHS Digital's processor (i.e. a sub-processor).</p>
	<p>NHS Digital is not the Supplier's processor for any information assets.</p> <p>The Parties are not Joint Controllers for any information assets.</p>
	<p>The Parties are Independent Controllers of the following Personal Data:</p> <p><i>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</i></p> <ul style="list-style-type: none"> <i>business contact details of Supplier Personnel for which the Supplier is the Controller,</i> <i>business contact details of any directors, officers, employees, agents, consultants and contractors of NHS Digital named in the Contract (excluding the Supplier Personnel), that are engaged in the performance of the NHS Digital duties under the Contract) for which the NHS Digital is the Controller (and their replacements).</i>
Duration of the Processing	<p><i>For the duration of the Call-off Contract only.</i></p>
Nature and purposes of the Processing	<p><i>The purpose of the Processing is:</i></p> <ul style="list-style-type: none"> <i>the development and safe delivery of transformation activity into live service from NHS Digital's prioritised backlog and from other transformation drivers.</i> <p><i>The nature of the Processing may include activities such as:</i></p> <ul style="list-style-type: none"> <i>collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation,</i> <i>use, alignment or combination, restriction,</i> <i>modification of data,</i>

Joint Schedule 11 (Processing Data)

Crown Copyright 2019

	<p><i>The following processing activities <u>shall not</u> occur unless specifically required in writing by NHS Digital:</i></p> <ul style="list-style-type: none"><i>disclosure by transmission, dissemination or otherwise making available; erasure or destruction of entire data set (whether or not by automated means) etc.</i>
Type of Personal Data	<p><i>NHS Digital information assets include datasets relating to employees, NHS staff, patients and the public, including the following broad categories:</i></p> <ul style="list-style-type: none"><i>Patient / citizen : demographics information, NHS number, name, address, postcode, date of birth, NI number, telephone number, email address, access and language preferences.</i><i>Patient / citizen: security and logon information.</i><i>Patient / citizen: clinical information, images, biometric data, clinical data (current and historic), communications.</i><i>NHS Digital staff: pay, contact details, employment information, logon and security information.</i><i>Wider NHS Staff : contact details, employment information, logon and security information, security information.</i><i>Supplier staff providing systems and services to NHS Digital and the wider NHS: business contact information, educational achievement, security information.</i> <p><i>Further details of the information assets hosted on the listed platforms are detailed in the NHS Digital Unified Registry.</i></p>
Categories of Data Subject	<p><i>Dependant on the platform, categories of data subject include:</i></p> <ul style="list-style-type: none"><i>NHS Digital staff (including volunteers, agents, and temporary workers).</i><i>Wider NHS staff (including volunteers, agents, and temporary workers).</i><i>Patients / citizens: residents of predominantly England, but also some data relating to devolved authorities. Supplier staff providing systems and services to NHS Digital and the wider NHS.</i>

<p>Plan for return and destruction of the data once the Processing is complete</p> <p>UNLESS requirement under Union or Member State law to preserve that type of data</p>	<p>The personal data will remain on NHS Digital controlled platforms and subject to NHS Digital security. No data will be removed by the Supplier from the NHS Digital controlled platforms.</p> <p>Exceptions:</p> <ul style="list-style-type: none">• Supplier may retain the business contact details of any directors, officers, employees, agents, consultants and contractors of NHS Digital named in the Contract (excluding the Supplier Personnel), that are engaged in the performance of the NHS Digital duties under the Contract) for which the NHS Digital is the Controller (and their replacements).• NHS Digital may retain the business contact details of Supplier Personnel for which the Supplier is the Controller.
--	--

Annex 2 - Joint Controller Agreement – NOT USED AT CALL-OFF START DATE

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of Paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and Paragraphs 7-27 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the Supplier/Relevant Authority:

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and
- (e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the

Supplier's/Relevant Authority's privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Law as against the relevant Party as Controller.

Undertakings of both Parties

The Supplier and the Relevant Authority each undertake that they shall:

- (a) report to the other Party every 3 months on:
 - (i) the volume of Data Subject Access Requests (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
 - (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
 - (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
 - (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
 - (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,that it has received in relation to the subject matter of the Contract during that period;
- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject before disclosing or transferring the Personal Data to the third party. For the avoidance of doubt to which Personal Data is transferred must be

subject to equivalent obligations which are no less onerous than those set out in this Annex;

- (e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
 - (i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information
 - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
 - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Law;
- (h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and
- (i) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable

Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as