

DATA PROCESSING AGREEMENT

between

(1) The NHS Commissioning Board (known as NHS England)

and

(2) The Health and Social Care Information Centre (known as NHS Digital)

## CONTENTS

CLAUSE	PAGE
1	DEFINITIONS AND INTERPRETATION ..... 1
2	SCOPE OF THIS AGREEMENT ..... 5
3	PROCESSING OF PERSONAL DATA ..... 5
4	TERM AND TERMINATION ..... 13
5	REMEDIES ..... <b>Error! Bookmark not defined.</b>
6	NOTICES ..... 13
7	GENERAL ..... 13
8	GOVERNING LAW AND JURISDICTION ..... 14

**THIS AGREEMENT** is effective from the 20<sup>th</sup> April 2020 and will be subject to review within six months of this date.

**BETWEEN:**

- (1) The **NHS Commissioning Board** of Quarry House, Leeds, LS2 7UE, known as NHS England (the **Customer**); and
- (2) **The Health and Social Care Information Centre** of 1 Trevelyan Square, Leeds, LS1 6AE, known as NHS Digital (the **Supplier**);

**BACKGROUND**

- (A) The Customer has appointed the Supplier to provide the Services (as defined below) under the Principal Agreement (as defined below) for the provision of an online consultation solution.
- (B) In performing the Services, the Supplier is required to process certain Personal Data (as defined below). The Customer has agreed to provide (or make arrangements for the provision of) such Personal Data to the Supplier for processing only in accordance with the terms of this Agreement from the date on which this Agreement is entered into (the **Commencement Date**).
- (C) The Supplier is pursuant to this Agreement giving direct assurances to the Customer with regard to how Personal Data is processed and safeguarded.
- (D) To the extent that the Principal Agreement (or other agreements in place with the Supplier) contains any provisions which govern the processing of Personal Data by the Supplier, the parties agree and acknowledge that the provisions of this Agreement shall prevail to the extent of such conflict or inconsistency. Save as set out here, the terms of the Principal Agreements shall apply unamended.

**IT IS AGREED** as follows:

**1 DEFINITIONS AND INTERPRETATION**

1.1 The following definitions shall apply in this Agreement:

**Controller** shall take the meaning given in the Data Protection Legislation;

**Data Guidance** means any applicable guidance, guidelines, direction or determination, framework, code of practice, standard or requirement regarding information governance, confidentiality, privacy or compliance with the Data Protection Legislation (whether specifically mentioned in this Agreement or not) to the extent published and publicly available or their existence or contents have been notified to the Supplier by the Customer and/or any relevant Regulatory or Supervisory Body. This includes but is not limited to guidance issued by NHS Digital, the National Data Guardian for Health & Care, the Department of Health

and Social Care, NHS England, the Health Research Authority, Public Health England, the European Data Protection Board and the Information Commissioner;

**Data Loss Event** means any event that results, or may result, in unauthorised processing of Personal Data held by the Supplier under this Agreement or Personal Data that the Supplier has responsibility for under this Agreement including without limitation actual or potential loss, destruction, corruption or inaccessibility of Personal Data, including any Personal Data Breach.

**Data Processing Services** means the data processing services described in the Annex to this Agreement;

**Data Protection Impact Assessment** means an assessment by the Customer of the impact of the envisaged processing on the protection of Personal Data;

**Data Protection Legislation** means (i) the DPA 1998 (ii) the GDPR, the LED and any applicable national Laws implementing them as amended from time to time (iii) the DPA 2018 (iv) all applicable Law concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations

**Data Protection Officer** shall take the meaning given in the Data Protection Legislation;

**Data Subject** shall take the meaning given in the Data Protection Legislation;

**Data Subject Access 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;

**DPA 1998** means the Data Protection Act 1998

**DPA 2018** means Data Protection Act 2018;

**EU** means the European Union;

**European Data Protection Board** has the meaning given to it in the Data Protection Legislation;

**GDPR** means the General Data Protection Regulation (Regulation (EU) 2016/679)

**Information Commissioner** means the independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals ico.org.uk and any other relevant data

protection or supervisory authority recognised pursuant to the Data Protection Legislation;

**Law** means any law or subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply;

**LED** means the Law Enforcement Directive (Directive (EU) 2016/680)

**Personal Data** shall take the meaning given in the Data Protection Legislation;

**Personal Data Breach** shall take the meaning given in the Data Protection Legislation;

**Principal Agreements** means collectively:

- Work packages relating to NHS App pursuant to the Provision of Services Agreements between the Supplier and the Customer (as amended from time to time);
- NHS App Directions dated 27 September 2018 (as amended from time to time), made pursuant to the Health and Social Care Act 2012;
- any amendments or replacements to the above; and
- Further instructions issued the Supplier by the Customer through the programme board and programme governance processes;

**Processor** shall take the meaning given in the Data Protection Legislation;

**Processing** and cognate terms shall have the meaning given in the Data Protection Legislation;

**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; and regularly assessing and evaluating the effectiveness of such measures;

**Regulatory or Supervisory Body** means any statutory or other body having authority to issue guidance, standards or recommendations with which the Supplier and/or Supplier Personnel must comply or to which it or they must have regard, including:

- (i) CQC;

- (ii) NHS Improvement;
- (iii) NHS England;
- (iv) the Department of Health and Social Care;
- (v) the National Institute for Health and Care Excellence;
- (vi) Healthwatch England and Local Healthwatch;
- (vii) Public Health England;
- (viii) the General Pharmaceutical Council;
- (ix) the Healthcare Safety Investigation Branch;
- (x) Information Commissioner;
- (xi) European Data Protection Board;

**Restricted Country** means any country which is not (i) a member of the European Economic Area; or (ii) the United Kingdom; as may be updated from time to time;

**Services** means the goods and/or services to be supplied by the Supplier under the Principal Agreement;

**Sub-processor** means any third party appointed to process Personal Data on behalf of the Supplier related to this Agreement;

**Supplier Personnel** means any and all persons employed or engaged from time to time in the provision of the Services and/or the processing of Personal Data whether employees, workers, consultants or agents of the Supplier or any subcontractor or agent of the Supplier.

**Working Day** means a day other than a Saturday, Sunday or bank holiday in England

1.1.1 reference to any legislative provision shall be deemed to include any statutory instrument, bye law, regulation, rule, subordinate or delegated legislation or order and any rules and regulations which are made under it, and any subsequent re- enactment, amendment or replacement of the same;

1.1.2 the Annex forms part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annex; and

- 1.1.3 references to clauses and Annexes are to clauses and Annexes to this Agreement.

## 2 SCOPE OF THIS AGREEMENT

- 2.1 In consideration of the sum of £1 (receipt of which the Supplier expressly acknowledges) and in consideration of the Customer agreeing to provide or procure the provision of Personal Data to the Supplier, the parties have agreed that:
  - 2.1.1 from the Commencement Date, the terms of this Agreement will apply to and govern all processing of Personal Data by the Supplier for the purposes described; and
  - 2.1.2 this Agreement is supplemental to other Agreements between the Customer and Supplier and, in the case of conflict or inconsistency between any of the provisions of this Agreement and the provisions other Agreements, the provisions of this Agreement shall prevail to the extent of such conflict or inconsistency in relation to processing activities described herein.
- 2.2 Compliance by the Supplier with the provisions of this Agreement shall be at no additional cost to the Customer.

## 3 PROCESSING OF PERSONAL DATA

- 3.1 The Parties acknowledge that for the purposes of the Data Protection Legislation and the delivery of the Data Processing Services, the Customer, acting jointly with the GP practices procuring the Supplier's Services, is the Controller and the Supplier is the Processor. A Joint Data Controller Agreement will be established between the Customer and the GP practices that will define the respective responsibilities of the Controller Parties in relation to processing of Personal Data under this agreement.
- 3.2 The Supplier shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.
- 3.3 The Supplier shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, include:
  - 3.3.1 a systematic description of the envisaged processing operations and the purpose of the processing;

- 3.3.2 an assessment of the necessity and proportionality of the processing operations in relation to the Data Processing Services;
  - 3.3.3 an assessment of the risks to the rights and freedoms of natural persons; and
  - 3.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 3.4 The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:
- 3.4.1 process that Personal Data only in accordance with the instructions set out in the Annex, unless the Supplier is required to do otherwise by Law. If it is so required, the Supplier shall promptly notify the Customer before processing the Personal Data unless prohibited by Law.
  - 3.4.2 ensure that it has in place Protective Measures to protect against a Data Loss Event having taken account of the:
    - 3.4.2.1 nature of the data to be protected;
    - 3.4.2.2 harm that might result from a Data Loss Event;
    - 3.4.2.3 state of technological development; and
    - 3.4.2.4 cost of implementing any measures.
  - 3.4.3 ensure that:
    - 3.4.3.1 the Supplier personnel do not process the Personal Data except in accordance with this Agreement (and in particular the Annex)
    - 3.4.3.2 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:
      - 3.4.3.2.1 are aware of and comply with the Supplier's duties under this clause;
      - 3.4.3.2.2 are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor that are in writing and are legally enforceable;



3.4.3.2.3 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 advance and in writing to do so by the Customer or as otherwise permitted by this Agreement.

3.4.3.2.4 have undergone adequate training in the use, care, protection and handling of Personal Data that enables them and the Supplier to comply with their responsibilities under the Data Protection Legislation and this Agreement. The Supplier shall provide the Customer with evidence of completion and maintenance of that training within three Working Days of request by the Customer.

3.4.4 not transfer Personal Data outside of a Restricted Country unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

3.4.4.1 The Customer or the Supplier has provided appropriate safeguards in relation to the transfer as determined by the Customer;

3.4.4.2 the Data Subject has enforceable rights and effective legal remedies;

3.4.4.3 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 Customer in meeting its obligations) and;

3.4.4.4 the Supplier complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data.

3.4.5. Unless otherwise directed by the Customer, the Supplier shall without charge and within five (5) Working Days securely delete any copies of Personal Data the Supplier holds from its computer, communications systems and devices and, if required by the Customer, return the Personal Data to the Customer (including Personal Data held manually and in an electronic format) after the earlier of:

- 3.4.5.1 termination of the Agreement; or
    - 3.4.5.2 where the Processing of the Personal Data by the Supplier is no longer required for the Supplier's performance of its obligations as described in the relevant agreement between a GP practice and eConsult.
  - 3.4.6 Where Personal Data has been deleted, the Supplier shall provide the Customer with evidence that the Personal Data has been securely deleted in accordance with Data Protection Legislation within seven (7) Working Days of deletion.
  - 3.4.7 Nothing in clause 3.5.5 shall require the Supplier to return or destroy any Personal Data that the Supplier is required to retain by Law.
- 3.5 Taking into account the state of the art, the cost 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, the Supplier shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, but not limited to, as appropriate:
  - 3.5.1 the pseudonymisation and encryption of Personal Data;
  - 3.5.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - 3.5.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
  - 3.5.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.
- 3.6 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Supplier must:
  - 3.6.1 notify the Customer in writing of the intended Sub-processor and processing;
  - 3.6.2 obtain the written consent of the Customer;
  - 3.6.3 with support from the Customer where required, work to ensure written agreements with all Sub-processors to provide a materially similar level of protection for the Personal Data as set out in this Agreement and

where possible include the benefits of third-party rights to the Customer to enforce the same, and this will be reviewed jointly by the Customer and Supplier within six months of this Agreement's Commencement Date; the requirements of this clause shall equally apply to Sub-processors of the Supplier; and

- 3.6.4 provide the Customer with such information regarding the Sub-processor as the Customer may reasonably require.
- 3.6.5 Clause 3.6.3 shall not require the Supplier to replicate clauses 5.2 and 5.3 of this Agreement in its agreement with any Sub-processor.
- 3.7 The Supplier shall ensure that the third party's access to the Personal Data terminates automatically on termination of this Agreement for any reason save that the Sub-processor may access the Personal Data in order to securely destroy it.
- 3.8 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.
- 3.9 Subject to clause 3.12, the Supplier shall notify the respective GP practice immediately if it:
  - 3.9.1 receives a Data Subject Access Request (or purported Data Subject Access Request) connected with Personal Data processed under this Agreement;
  - 3.9.2 receives a request to rectify, block or erase any Personal Data connected with Personal Data processed under this Agreement;
  - 3.9.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation connected with Personal Data processed under this Agreement;
  - 3.9.4 receives any communication from the Information Commissioner or any other Supervisory or Regulatory Body connected with Personal Data processed under this Agreement;
  - 3.9.5 receives a request from any third party for disclosure of Personal Data connected with this Agreement;
  - 3.9.6 becomes aware an actual or suspected Data Loss Event;
  - 3.9.7 should any notifications referred to in clauses 3.9.4 – 3.9.6 have regard to Personal Data held by multiple GP practices, the Supplier, if it is aware it is the case, shall also immediately notify the Customer.

- 3.10 This notification shall be given by emailing the original request and any subsequent communications to the GP practice's or Customer's Data Protection Officer (and Sub-Processors shall similarly notify the Supplier's Data Protection Officer).
- 3.11 The Customer shall procure, via its Joint Controller Agreement, that the GP practices, as Controllers, shall comply with Data Protection Legislation and bear responsibility for responding substantively to the communications listed at clause 3.9. The Supplier shall not respond substantively to the communications listed at clause 9 save that it may respond to a Regulatory or Supervisory Body following prior consultation with the Customer.
- 3.12 The Supplier's obligation to notify under clause 3.9 shall include the prompt provision of further information to the Customer or GP practice (as the case may be) in phases, as details become available.
- 3.13 Taking into account the nature of the processing, the Supplier shall provide the Customer or GP practice with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 3.9 (and insofar as possible within the timescales reasonably required by the Customer) including by promptly providing:
- 3.13.1 full details and copies of the complaint, communication or request;
  - 3.13.2 such assistance as is reasonably requested by the GP practice to enable the Customer or GP practice to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation and the Supplier's Sub-processor shall similarly assist the Supplier to enable it to comply with this clause;
  - 3.13.3 such assistance as is reasonably requested by the GP practice to enable the GP practice to comply with other rights granted to individuals by the Data Protection Legislation including the right of rectification, the right to erasure, the right to object to processing, the right to restrict processing, the right to data portability and the right not to be subject to an automated individual decision (including profiling);
  - 3.13.4 the GP practice, at its request, with any Personal Data it holds in relation to a Data Subject;
  - 3.13.5 assistance as requested by the GP practice or Customer following any Data Loss Event;
  - 3.13.6 assistance as requested by the GP practice or Customer in relation to informing a Data Subject about any Data Loss Event, including communication with the Data Subject;

- 3.13.7 assistance as requested by the GP practice or Customer with respect to any request from the Information Commissioner's Office, or any consultation by the GP practice or Customer with the Information Commissioner's Office;
  - 3.13.8 the GP practice with any copies of requests from Data Subjects seeking to exercise their rights under the Data Protection Legislation. Such requests must be sent, to the GP practice's Data Protection Officer immediately, and in no longer than one Working Day of receipt by the Supplier (and similarly Sub-processors should notify the Supplier within one Working Day of their receipt of such requests).
- 3.14 The Supplier shall allow for audits of its delivery of the Data Processing Services by the Customer or the Customer's designated auditor.
- 3.15 The Supplier shall provide the Customer with evidence to demonstrate compliance with all of its obligations under this Agreement and the relevant Data Protection Legislation.
- 3.16 The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation and shall communicate to the Customer the name and contact details of its Data Protection Officer.
- 3.17 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Agreement, the Data Protection Legislation and Data Guidance. The Supplier must create and maintain a record of all categories of data processing activities carried out under this Agreement, containing:
  - 3.17.1 the categories of processing carried out under this Agreement;
  - 3.17.2 where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards;
  - 3.17.3 a general description of the Protective Measures taken to ensure the security and integrity of the Personal Data processed under this Agreement; and
  - 3.17.4 a log recording the processing of Personal Data in connection with this Agreement comprising, as a minimum, details of the Personal Data concerned, how the Personal Data was processed and where the Personal Data was processed.

- 3.18 The Supplier shall ensure that the record of processing maintained in accordance with clause 3.17 is provided to the Customer within five Working Days of a written request from the Customer.
- 3.19 This Agreement does not relieve the Supplier from any obligations conferred upon it by the Data Protection Legislation.
- 3.20 The Parties agree to take account of any guidance issued by the Information Commissioner. The Customer may on not less than 30 Working Days' notice to the Supplier amend this Data Processing Agreement to ensure that it complies with any guidance issued by the Information Commissioner.
- 3.21 The Customer may, at any time on not less than 30 Working Days' notice, revise this clause by adding to it 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 Agreement).
- 3.22 The Supplier warrants and undertakes that it will deliver the Data Processing Services in accordance with all Data Protection Legislation, any Data Guidance and this Agreement and in particular that it has in place Protective Measures that are sufficient to ensure that the delivery of the Data Processing Services complies with the Data Protection Legislation and ensures that the rights of Data Subjects are protected. The Supplier shall not do or omit to do anything that will put the GP practices or Customer in breach of the Data Protection Legislation or the Data Guidance.
- 3.23 The Customer warrants and undertakes that it will comply with all Data Protection Legislation and will put in place Joint Data Controller Agreements with those GP practices using the Supplier's services to confer relevant data protection obligations onto them.
- 3.24 The Supplier must assist the Customer in ensuring compliance with the obligations set out at Article 32 to 36 of the GDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to the Supplier.
- 3.25 The Supplier must take prompt and proper remedial action regarding any Data Loss Event on their part, with the support of the Customer.
- 3.26 The Supplier must assist the Customer by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the GP practices' obligation to respond to requests for exercising rights granted to individuals by the Data Protection Legislation.

## 4 **TERM AND TERMINATION**

- 4.1 This Agreement shall commence on the Commencement Date. Unless terminated in accordance with this clause, this Agreement shall automatically terminate, with respect to an individual GP practice, on the expiry of the GP practice's agreement with eConsult.
- 4.2 Without affecting any other right or remedy available to it, the Customer may immediately terminate this Agreement by notice in writing to the Supplier if the Supplier commits a material breach of any provision of this Agreement or the Supplier repeatedly breaches any of the provisions of this Agreement.
- 4.3 On termination of this Agreement:
- 4.3.1 any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of this Agreement which existed at or before the date of termination, shall not be affected;
  - 4.3.2 the provisions of this Agreement which place obligations on the Supplier in respect of the processing of Personal Data shall continue in force and effect until such time as all Personal Data (including all copies thereof) has either been returned and/or destroyed in accordance with the foregoing sub-clause (unless otherwise strictly required by Law);
  - 4.3.3 without prejudice to the foregoing sub-clause, the provisions of this Agreement that expressly or by implication are intended to come into or continue in force on or after termination of this Agreement shall remain in full force and effect.

## 5 **NOTICES**

- 5.1 Any notice given to a party under or in connection with this Agreement shall be in writing in the English language and shall be sent by email to the other party.
- 5.2 Any notice validly given in accordance with the foregoing clause shall be deemed to have been received the following Working Day.

## 6 **GENERAL**

- 6.1 The Supplier shall not assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any or all of its rights and obligations under this Agreement without the prior written consent of the Customer, such consent shall not be unreasonably withheld or delayed.

- 6.2 The Supplier may agree variations to this Agreement by agreement with the Customer (or a body nominated by the Secretary of State for Health and Social Care for the purpose). Such changes shall not take effect until published by NHSX on its website (or any other site nominated by the Secretary of State for Health and Social Care for the purpose). No variation of this Agreement shall be effective unless it is in writing and signed by the parties to this Agreement. Any variations agreed by the Supplier shall be flowed down to its Sub-processors.
- 6.3 Subject to clause 7.2, the Supplier's undertakings in this Agreement are irrevocable.
- 6.4 This Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

## **7 GOVERNING LAW AND JURISDICTION**

- 7.1 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the Law of England.
- 7.2 Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims), provided that nothing in this clause shall prevent a party from enforcing any judgement obtained in the court of England and Wales in any other court with jurisdiction over the other party.

**THIS AGREEMENT** has been entered into on the date stated at the beginning of it.



## ANNEX – DATA PROCESSING SERVICES

1. The Supplier shall comply with any further written instructions with respect to processing by the Customer.
2. Any such further instructions shall be incorporated into this Annex.

Description	Details
Subject matter of the processing	<i>GP Practices deliver public health care within England. The Supplier will enable integration of eConsult's online consultation solution with the NHS App. eConsult enables practices to support the delivery of such services remotely. During the course of the provision of the Services, patients will generate further additional Personal Data (including Special Category data), which shall also be classed as Personal Data, via the NHS App. The Supplier will facilitate transmission of the personal data between the NHS App and eConsult. The Customer, acting jointly with GP practices, shall be the Controller. The Supplier will be a Processor.</i>
Duration of the processing	<i>The processing is effective for the periods set out in the relevant Principal Agreements.</i>
Nature and purpose of the processing	<p><i>In relation to the online consultation service:</i></p> <ul style="list-style-type: none"> <li>• <i>Transmission of data collected by the NHS App in relation to eConsult to eConsult Health Limited</i></li> <li>• <i>Transmission of data generated by eConsult Health limited to the patient, via the NHS App</i></li> </ul> <p><i>All data relating to the eConsult service is processed within the UK and EEA. This includes all Sub-processor data.</i></p> <p><i>Pursuant to clause 3.6.2 the Customer has consented to the following Sub-processors:</i></p> <ul style="list-style-type: none"> <li>• <i>service providers acting as Sub-processors who provide web application firewall services.</i></li> </ul>
Type of Personal Data	<i>Patients / Patients' representatives/guardians: data provided and requested by the provision of the eConsult Health Limited online consultation service to patients on behalf of GPs, to include details medical symptoms and conditions, and triage information</i>
Categories of Data Subject	<i>Registered patients of the Customer. Patients / Patients' Representatives / Guardians, Practice Users, persons working within the wider NHS and social care system.</i>
Plan for return of the data once the Processing is complete unless requirement under union or	<i>Personal Data will be retained only for: a) the duration of the Principal Agreement (unless the Customer has requested the secure deletion of such data); or b) if applicable, such other shorter period provided for in the relevant Principal Agreement or otherwise agreed between the Customer and the Supplier.</i>

member state law to preserve that type of data	
Standards and Governance	<p><i>The Supplier shall comply with the following standards, guidance and governance unless otherwise agreed expressly in writing with the Customer by naming the relevant item and expressly disapplying them, in relation to its provision of the public services, as updated from time to time:</i></p> <ul style="list-style-type: none"> <li>• <i>UK Information Commissioner Data Guidance;</i></li> <li>• <i>DSP Toolkit, further information is available at : <a href="https://www.dsptoolkit.nhs.uk/">https://www.dsptoolkit.nhs.uk/</a></i></li> <li>• <i>Confidentiality: NHS Code of Practice, further information is available at : <a href="https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice">https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice</a></i></li> <li>• <i>applicable guidance of the National Data Guardian, in accordance with the Health and Social Care (National Data Guardian) Act 2018, further information is available at : <a href="http://www.legislation.gov.uk/ukpga/2018/31/contents/enactedhttps://www.gov.uk/government/organisations/national-data-guardian">http://www.legislation.gov.uk/ukpga/2018/31/contents/enactedhttps://www.gov.uk/government/organisations/national-data-guardian</a></i></li> <li>• <i>the Network and Information Systems Regulations 2018, to the extent applicable to its provision of the Services.</i></li> <li>• <i>the Information Standards, to the extent applicable to its provision of the Services, further information is available at : <a href="https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections">https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections</a></i></li> </ul> <p><i>For the avoidance of doubt, Data Subjects shall be able to receive the Data Processing services without being required to opt out of the application of these standards and guidance. Data Subjects cannot be required by the Supplier to opt out of the application of these standards and guidance as part of their receipt of the Data Processing services.</i></p>
Supplier's Data Protection Officer	Catherine Nicholson

Signed by **Matt Neligan** for and on behalf of  
**NHS ENGLAND:**



\_\_\_\_\_  
Matt Neligan

\_\_\_\_\_  
19/05/2020

Signature of Director

Name of Director (PRINT)

Date

Signed by **Jackie Gray** for and on behalf of  
**NHS DIGITAL:**



\_\_\_\_\_  
Jackie Gray

\_\_\_\_\_  
13 May 2020

Signature of Director

Name of Director (PRINT)

Date