Data Processing Addendum

BACKGROUND

1. This Data Processing Addendum ("**DPA**") supplements the Master Services and Software Agreement between the Customer and the Supplier, or other agreement as expressly agreed between the Customer and Supplier governing the Customer's use of the Services (the "**Master Agreement**").

2. This DPA is an agreement between and Customer the Supplier under the Master Agreement.

3. This DPA applies when Customer Data is processed by the Supplier. In this context, the Supplier will act as Processor, and the Customer will be the Controller of Customer Data.

4. This DPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement shall apply to the interpretation of this DPA. In the case of conflict or ambiguity between any provision of this DPA and the provisions of the Master Agreement, the provisions of this DPA will prevail.

5. In the event that the EU GDPR applies to the Processing activities between the Customer and the Supplier, all references to the UK GDPR in this DPA shall be replaced with references to EU GDPR.

6. The Supplier reserves the right to update this DPA from time to time when required by any Data Protection Laws or relevant domestic law.

AGREED TERMS

1 Definitions and Interpretation

The following definition and rules of interpretation apply to this DPA.

Applicable Law	means the applicable law as defined in the Master Agreement;
Controller	has the meaning given in applicable Data Protection Laws from time to time;
Customer	means the relevant legal entity as defined in the Master Agreement;
Customer Personal Data	means any Personal Data that is uploaded to the Services under the Customer's Idox Account;
Data Protection Laws	means all applicable data protection and privacy laws in force from time to time in the UK including without limitation the EU GDPR, the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) ("DPA 2018"); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications);
EU GDPR	means the General Data Protection Regulation, Regulation (EU) 2016/679)
EEA	the European Economic Area

Data Subject	the identified or identifiable living individual to whom the Customer Personal Data relates
UK GDPR	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.
International Organisation	has the meaning given in applicable Data Protection Laws from time to time;
Personal Data	means any information relating to an identified or identifiable living individual that is processed by the Supplier on behalf of the Customer as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual
Personal Data Breach	a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Customer Personal Data
Processing, processes, processed, process:	any activity that involves the use of the Customer Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Customer Personal Data or on sets of the Customer Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Customer Personal Data to third-parties.
Processor	has the meaning given in applicable Data Protection Laws from time to time;
Services	means the services to be provided by the Supplier to the Customer under the Master Agreement; and
Sub-Processor	means any Processor engaged by the Supplier (or by any other Sub-Processor) for carrying out any processing activities in respect of the Customer Personal Data on behalf of the Customer.
Supplier	means the relevant legal entity and wholly owned subsidiary of Idox plc as set out in any quotation issued by the Supplier and accepted by you, as the Customer in the Master Agreement.

2 Customer's compliance with Data Protection Laws

2.1 The parties agree that the Customer is the Controller and that the Supplier is the Processor for the purposes of processing Customer Personal Data pursuant to this DPA.

2.2 The Customer shall, at all times, comply with all Data Protection Laws in connection with the processing of Customer Personal Data.

2.3 The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Laws, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Supplier.

2.4 Annex A to this DPA describes the subject matter, duration, nature and purpose of the processing and the Customer Personal Data categories and Data Subject types in respect of which the Supplier may process the Customer Personal Data to fulfil the Services.

2.5 The Customer shall ensure all instructions given by it to the Supplier in respect of Customer Personal Data (including the terms of this DPA) shall at all times be in accordance with Data Protection Laws. Nothing in this DPA relieves the Customer of any responsibilities or liabilities under any Data Protection Laws.

3 Supplier's compliance with Data Protection Laws

3.1 The Supplier shall process Customer Personal Data in compliance with the obligations placed on it under Data Protection Laws and the terms of this DPA.

3.2 The Supplier will ensure that all of its employees:

a) are informed of the confidential nature of the Customer Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Customer Personal Data;

b) have undertaken training on the Data Protection Laws and how it relates to their handling of the Customer Personal Data and how it applies to their particular duties; and

c) are aware both of the Supplier's duties and their personal duties and obligations under the Data Protection Laws and this DPA.

4 Instructions

4.1 The Supplier shall only process Customer Personal Data in accordance with Annex A to this DPA, except to the extent:

4.1.1 that alternative processing instructions are agreed between the parties in writing; or

4.1.2 otherwise required by Applicable Law (and shall inform the Customer of that legal requirement before processing, unless Applicable Law prevents it doing so on important grounds of public interest).

4.2 If the Supplier believes that any instruction received by it from the Customer is likely to infringe the Data Protection Laws it shall be entitled to cease to provide the relevant Services until the parties have agreed appropriate amended instructions which are not infringing.

5 Security

5.1 The Supplier shall implement and maintain the technical and organisational measures set out in Section 2 of Annex A to this DPA to protect Customer Personal Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access.

5.2 The Supplier must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

5.2.1 the pseudonymisation and encryption of Customer Personal Data;

5.2.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.2.3 the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and

5.2.4 a process for regularly testing, assessing and evaluating the effectiveness of the security measures

5.3 During the period in which the Supplier processes any Customer Personal Data, the Customer shall undertake a documented assessment at least every 12 months of whether the security measures implemented in accordance with paragraph 5.1 of this DPA are sufficient (taking into account the state of technical development and the nature of processing) to protect the Customer Personal Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access. The Customer shall notify the Supplier of full details of the assessment and its outcome and of any additional measures the Customer believes are required as a result of the assessment. The Supplier shall not be obliged to implement any further or alternative security measures except as agreed as a binding variation of this DPA.

6 Sub-processing and personnel

6.1 The Supplier shall:

6.1.1 not permit any processing of Customer Personal Data by any Sub-Processor without the prior specific written authorisation of the Customer;

6.1.2 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Customer Personal Data, ensure each Sub-Processor is appointed under a binding written contract containing materially the same obligations as under this DPA (including those relating to sufficient guarantees to implement appropriate technical and organisational measures) and ensure each such Sub-Processor complies with all such obligations;

6.1.3 remain fully liable to the Customer under this DPA for all the acts and omissions of each Sub-Processor as if they were its own; and

6.1.4 ensure that all persons authorised by the Supplier or any Sub-Processor to process Customer Personal Data are subject to a binding written contractual obligation to keep the Customer Personal Data confidential.

7 Further Sub-Processors

The Customer shall reply to any communication from the Supplier requesting any further prior specific authorisation of a Sub-Processor pursuant to paragraph 6.1.1 of this DPA promptly and in any event within 10 days of request. The Customer shall not unreasonably withhold, delay or condition any such authorisation.

8 Complaints, data subject requests and third-party rights

8.1 The Supplier will take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

a) the rights of Data Subjects under the Data Protection Laws, including, but not limited to, subject access rights, the rights to rectify, port and erase Customer Personal Data, object to the processing and automated processing of Customer Personal Data, and restrict the processing of Customer Personal Data; and

b) information or assessment notices served on the Customer by the Information Commissioner's Office under the Data Protection Laws.

8.2 The Supplier must notify the Customer as soon as reasonably practicable in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Customer Personal Data or to either party's compliance with the Data Protection Laws.

8.3 The Supplier must notify the Customer within 2 days if it receives a request from a Data Subject for access to their Customer Personal Data or to exercise any of their other rights under the Data Protection Laws.

8.4 The Supplier will give the Customer its co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

8.5 The Supplier must not disclose the Customer Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic or EU law.

9 International transfers

The Supplier shall not transfer, or otherwise directly or indirectly disclose, any Customer Personal Data in or to countries outside the EEA without the prior written authorisation of the Customer except where required by Applicable Law.

10 Audits and processing

The Supplier shall, in accordance with Data Protection Laws, make available to the Customer on request such information that is in its possession or control as is necessary to demonstrate the Supplier's compliance with the obligations placed on it under this DPA and to demonstrate compliance with the obligations on each party imposed by the Data Protection Laws, and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose subject to a maximum of one audit request in any 12 month period under this paragraph 10. The Supplier shall, however, be entitled to withhold information where it is commercially sensitive or confidential to it or its other customers.

11 Personal data breach

11.1 The Supplier shall notify the Customer without undue delay and in writing on becoming aware of any Customer Personal Data Breach in respect of any Customer Personal Data.

11.2 Where the Supplier aware of a Customer Personal Data Breach it will, without undue delay, provide the Customer with the following written information:

a) description of the nature of the Customer Personal Data Breach including the categories of in-scope Customer Personal Data and approximate number of both Data Subjects and the Customer Personal Data records concerned;

b) the likely consequences; and

c) a description of the measures taken or proposed to be taken to address the Customer Personal Data Breach, including measures to mitigate its possible adverse effects.

11.3 As soon as reasonably practicable following any accidental, unauthorised or unlawful Customer Personal Data processing or Customer Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Supplier will reasonably co-operate with the Customer at in the Customer's handling of the matter, including but not limited to:

c) assisting with any investigation;

d) facilitating interviews with the Supplier's employees;

e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Customer Personal Data Breach or accidental, unauthorised or unlawful Customer Personal Data processing.

11.4 The Supplier will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Customer Personal Data and/or a Customer Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic or EU law.

12 Deletion/return

12.1 On the end of the provision of the Services relating to the processing of Customer Personal Data (the **Processing End Date**), at the Customer's cost and expense and the Customer's option, the Supplier shall either return all of the Customer Personal Data to the Customer or securely dispose of the Customer Personal Data (as far as reasonably practicable) except to the extent that any Applicable Law requires the Supplier to store such Customer Personal Data.

12.2 To the extent the Customer has not notified the Supplier within 10 days of the Processing End Date that it requires the return of any Customer Personal Data the Supplier is irrevocably authorised to securely dispose (as far as reasonably practicable) of the Customer Personal Data at the Customer's cost and expense.

12.3 The Supplier shall confirm in writing whether or not it has complied with its obligations to dispose of the Customer Personal Data under paragraph 12.1 of this DPA within 10 working days after it completes the deletion or return.

13 Term and Termination

13.1 This DPA will remain in full force and effect so long as:

13.1.1 the Master Agreement remains in effect or;

13.1.2 the Supplier retains any of the Customer Personal Data related to the Master Agreement its in possession.

13.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect the Customer Personal Data will remain in full force and effect.

13.3 If a change in any Data Protection Laws prevents either party from fulfilling all or part of its Master Agreement obligations, the parties may agree to suspend the processing of the Customer Personal Data until that processing complies with the new requirements.

Annex A

Section 1—Data processing details

Processing of the Personal Data by the Supplier under this DPA shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in this Section 1 of Annex A

1 Purpose of the processing:

The purpose of the Processing under this DPA is the provision of the Services initiated by Customer from time to time.

2 Duration of the processing:

The duration of the processing is the duration of the Master Agreement

3 Nature of the processing:

The processing may include the collection, recording and storing of Customer Personal Data as further described in the Master Agreement and initiated by Customer from time to time

4 Type of Personal Data:

The types of personal data may include names, addresses and all other personal data provided to the processor by way of the customers use of the Services.

5 Categories of Data Subjects:

The data subjects could include Customer's customers, employees, suppliers and end users.

Section 2—Minimum technical and organisational security measures

The Supplier shall implement and maintain the following technical and organisational security measures to protect the Personal Data:

- **Infrastructure.** The Supplier stores all production data in physically secure locations within the United Kingdom and EEA.
- **Environmental Redundancy.** All environmental equipment and facilities have preventative maintenance procedures.
- **Power.** Mains power protection is provided during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power and controlled, safe shutdown of systems.
- **Server Operating Systems.** All IT infrastructure utilises industry standard enterprise level Operating Systems which are regularly patched in accordance with the software vendors recommendation. All systems are protected with anti-virus, anti-malware and anti-ransomware software, as appropriate.
- **Businesses Continuity.** The Supplier maintains a cloud-based backup and replication systems and regularly plans and tests its business continuity/disaster recovery procedures.
- **Data Transmission.** To prevent data from being read, copied, altered or removed without authorisation the Supplier encrypts and/or password protects all transmissions containing Personal Data.
- **Encryption Technologies.** The Supplier uses AES and/or HTTPS encryption (also referred to as a SSL or TLS connection) as appropriate.