

**MEMORANDUM OF UNDERSTANDING for Provision of GOV.UK Platform as a Service**

**Dated** [insert date]

**BETWEEN**

- (1) **THE MINISTER FOR THE CABINET OFFICE**, acting through **THE GOVERNMENT DIGITAL SERVICE** of White Chapel Building, 10 Whitechapel High Street, London E1 8DX (“**the Authority**” or “**GDS**”)

and

- (2) [insert TENANT BODY details] (“**the Tenant**”),

each a “**Party**” and collectively the “**Parties**”.

**WHEREAS**

The Tenant wishes to enter this Memorandum of Understanding (“**MOU**”) with GDS for the provision of the GOV.UK Platform where GDS shall act as central purchasing body:

- A. GDS acts as a central purchasing body within the meaning of regulation 37 of the Public MOUs Regulations 2015 or regulation 38 of the Public MOUs (Scotland) Regulations (as appropriate). In particular, GDS acquires services intended for contracting authorities.
- B. Under regulation 37(4) of the Public MOUs Regulations 2015 or regulation 38(4) of the Public MOUs (Scotland) Regulations 2015 (as appropriate), the Tenant fulfils its obligations under the Public MOUs Regulations 2015 or Public MOUs (Scotland) Regulations 2015 (as appropriate) when it acquires services from GDS as a central purchasing body.
- C. Schedule 1 covers the Processing of Personal Data, the relationship between one Crown body (GDS) and a non-Crown body where one Party is the Controller and the other party is a Processor. It is not designed to cover joint controllers of personal data for which an alternative arrangement will be required. Article 28 of the GDPR and section 59 of the Data Protection Act 2018 require there to be a contract in place between controllers and processors. Accordingly Schedule 1 shall be contractually binding. Schedule 1 is not a public service contract and so not in scope of the Public MOUs Regulations 2015.
- D. Schedule 2 sets out the basis on which the Tenant pays GDS for specific services that GDS acquires for its use. Schedule 2 is profit neutral and its purpose is to achieve GOV.UK PaaS objectives in the public interest. Schedule 2 shall not be legally binding.

## THE PARTIES HEREBY AGREE:

### 1. DEFINITIONS AND INTERPRETATION

1.1. In this MOU except where the context otherwise requires, the following words and expressions shall have the following meanings:

**“Admin Personal Data”** means Personal Data that GDS controls in order to administer GOV.UK PaaS, about the Tenant’s employees and or authorised users who are authorised administrators of GOV.UK PaaS for the Services.

**“Authority Personnel”** means Authority staff and sub-contractor staff.

**“Charges”** means the charges for the Services as specified in Schedule 3;

**“Confidential Information”** means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;

**“Controller”** takes the meaning given in the GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the DPA 2018 applies, the meaning in that Part if different.

**“Data Breach”** is a breach of Data Protection Legislation.

**“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”** takes the meaning given in the GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the DPA 2018 applies, the meaning in that Part if different.

**“Data Subject”** takes the meaning given in the GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the DPA 2018 applies, the meaning in that Part if different.

**“Dispute”** means any dispute, difference or question of interpretation arising out of or in connection with this MOU, including any dispute, difference or question of interpretation relating to the Services.

**“DPA 2018”** means the Data Protection Act 2018.

**“FOIA”** means the Freedom of Information Act 2000 and any subordinate legislation made under that act from time to time, together with any guidance and/or codes of practice issued by the Information Commissioner or the government department responsible for such legislation.

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

**“GDS”** means the Government Digital Service, which is a part of the Cabinet Office.

**“GOV.UK PaaS”** means GOV.UK Platform as a Service, the HM Government’s digital platform component that enables hosting of government apps/services.

**“Information”** means any information in any written, electronic or other tangible form either: (a) disclosed to one Party by or on behalf of the other Party; or (b) obtained by a Party in connection with this MOU. For the avoidance of doubt, Information shall include Personal Data, any information covered by any Government security classification, any technical information, know-how, trade secrets and other information in any form or medium whether disclosed orally, in writing or in any other tangible form, together with any reproductions of such Information (whether in whole or in part) in any form or medium.

**“ICO”** means the Information Commissioner Office as the independent regulatory office in charge of upholding information rights in the interest of the public.

**“Intellectual Property Rights”** means patents, rights to inventions, copyright and related rights, trade marks, business names and domain names, rights in get-up, goodwill and the right to sue for passing off, rights in designs, database rights, rights in computer software, rights to and in know-how and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

**“Law”** means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply. Any reference in this MOU which immediately before Exit Day is a reference to (as it has effect from time to time):

- (i) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 and which shall be read on and after Exit Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and

- (ii) any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred.

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

**“Loss”** means any loss, liability, damage, cost or expense (including reasonable legal expenses).

**“PaaS”** means Platform as a Service being the Services described in Schedule 1;

**“Personnel”** means directors, officers, employees, agents, consultants and contractors.

**“Personal Data”** takes the meaning given in the GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the DPA 2018 applies, the meaning in that Part if different.

**“Personal Data Breach”** takes the meaning given in the GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the DPA 2018 applies, the meaning in that Part if different.

**“Processor”** takes the meaning given in the GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the DPA 2018 applies, the meaning in that Part if different.

**“Processing”** takes the meaning given in the GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the DPA 2018 applies, the meaning in that Part if different.

**“Processor Personnel”** means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this MOU;

**“Protective Measures”** mean 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 the such measures adopted by it.

**“Representative”** means any of the Tenant’s employees, directors, agents or subcontractors.

**“Services”** means the hosting by GDS on GOV.UK PaaS as described in Schedule 3.

**“Service Data”** means any data, other than personal data as defined in applicable Data Protection Legislation, that the Tenant places on GOV.UK PaaS as part of their Service or

Services, including but not limited to, application source code; application assets and other application resources.

**“Services Personal Data”** means any Personal Data that the Tenant places on GOV.UK PaaS as part of the Services.

**“Subject Request”** means a request made by, or on behalf of, a Subject in accordance with rights granted pursuant to the Data Protection Legislation in respect of their Personal Data.

**“Sub-processor”** means any third Party appointed to process Personal Data on behalf of that Processor related to this contract. Sub processors are listed in Annex 2

**“Term”** has the meaning set out in Clause 2.

**“Tenant”** means the purchaser of the Services and the owner of apps/services relevant to this MOU hosted on GOV.UK PaaS.

**“VAT”** means value added tax or goods and services tax or any equivalent tax chargeable in the UK.

## **2. BASIS OF MOU AND TERM**

2.1. The Parties do not intend to create legal relations except with respect to Schedule 1.

2.2. This MOU shall come into effect on the date where both Parties have signed, which may be in counter-parts, and continue until the later of the:

- (a) full delivery of the Services; and
  - (b) the full and final payment of the Charges to GDS by the Tenant; or
  - (c) termination of this MOU in accordance with Clause 11 or elsewhere in this MOU.
- (the **Term**).

## **3. SUPPLY OF SERVICES**

3.1. The Authority shall supply the Services to the Tenant for the Term.

3.2. The Tenant shall:

- (a) co-operate with GDS in all matters relating to the Services;
- (b) provide GDS with such Information and materials as GDS may reasonably require to provide the Services and ensure that such Confidential Information is complete and accurate in all respects;
- (c) obtain and maintain all necessary licences, permissions and consents that may be required for the Services before the date on which the Services are to start.

#### **4. CHARGES AND PAYMENT TERMS**

- 4.1. The Charges for the Services shall be as set out in Schedule 2 in respect of the supply of the Services. Unless otherwise agreed in writing between the Parties, the Charges shall include every cost and expense of GDS directly or indirectly incurred in connection with the performance of the Services.
- 4.2. All amounts payable by the Tenant under this MOU are exclusive of any VAT chargeable at the prevailing rate and of any other applicable duties or taxes. Where any taxable supply for VAT purposes is made under this MOU by GDS to the Tenant, the Tenant shall, on receipt of a valid VAT invoice from GDS, pay to GDS such additional amounts in respect of VAT as are chargeable on the supply of the Services at the same time as payment is due for the supply of the Services.

#### **5. VARIATION OF THE MOU**

- 5.1. Subject to paragraph 2.13 of Schedule 1, either Party may request a variation to this MOU which is only effective if agreed in writing and signed by both Parties.

#### **6. CONFIDENTIALITY AND DISCLOSURE OF INFORMATION**

- 6.1. If either Party receives any enquiry, complaint, claim or threat of action from a third party including, but not limited to, claims made by a supplier or requests for information made under FOIA in relation to this MOU, the matter shall be promptly referred to the Data Protection Officer of each Party (or its nominated representatives). No action shall be taken in response to any such enquiry, complaint, claim or action, to the extent that such response would adversely affect this MOU, without the prior approval of the other Party concerned (or its nominated representatives).

#### **7. INTELLECTUAL PROPERTY RIGHTS**

- 7.1. All pre-existing Intellectual Property Rights belonging to or licenced to a Party or other Intellectual Property Rights created outside the scope of the Services is and shall remain the exclusive property of the party owning it and except as expressly provided in this MOU, no Party shall acquire any rights in or to such Intellectual Property rights.

#### **8. PERSONAL DATA**

- 8.1. The Parties agree to the provisions set out in Schedule 1.

## **9. TENANT'S OBLIGATIONS**

9.1. The Tenant's Responsibilities are described in Schedule 4.

9.2. The Tenant shall:

- (i) co-operate with GDS in all matters relating to the Services;
- (ii) provide GDS with such Information and materials as GDS may reasonably require to provide the Services;
- (iii) obtain and maintain all necessary licences, permissions and consents that may be required for the Services before the date on which the Services are to start.

## **10. LIABILITY**

10.1. Nothing in these Conditions shall limit or exclude a Party's liability for:

- (i) any liability which cannot be limited or excluded by applicable law including for death or personal injury caused by negligence or for fraud or fraudulent misrepresentation; or

10.2. Nothing in this MOU shall prejudice the ability of GDS in carrying out its operational duties and no liability shall be incurred by GDS under this MOU or otherwise should GDS be unable to perform the Services and/or its other obligations under this MOU at any time.

10.3. Subject to Clause 10.1, GDS's total liability to the Tenant whether in contract, tort (including negligence), breach of statutory duty, howsoever arising under or in connection with the MOU, shall in no circumstances exceed the Charges.

10.4. Subject to Clause 10.1, GDS shall under no circumstances be liable to the Tenant, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, for any loss arising under or in connection with this MOU in respect of any:

- (a) (i) loss of profit; (ii) loss of sales or business; (iii) loss of agreements or contracts; (iv) damage to or loss of use or corruption of software, data or information; (v) loss of or damage to goodwill; or (vi) loss of anticipated savings or any other sort of economic loss (in each case whether direct or indirect);
- (b) any indirect or consequential loss.

## **11. TERMINATION**

11.1. This MOU shall commence on the date this MOU has been signed by both Parties and shall continue, unless terminated earlier in accordance with clause 11.2. Unless terminated earlier

in accordance with clause 11.2, the MOU shall terminate automatically without notice at the end of the Term.

11.2. A Party may terminate this MOU by giving the other Party at least three months' notice in writing at any time.

11.3. Upon termination, the Processor shall comply with any direction given by the Controller in relation to deletion or return of Personal Data under paragraph 2.4.5 of Schedule 1 save as otherwise required by law.

11.4. The Parties should give due consideration to whether any further Processing of the Personal Data is compliant with the Data Protection Legislation.

## 12. DISPUTES

12.1. Subject to clause 13.3, if either Party has any issues, concerns or complaints, that Party shall notify the other Party and the Parties shall, acting in good faith, seek to resolve the issue by negotiations between themselves. If the issue cannot be resolved within 7 days,

- (a) if the matter is related to a Data protection matter, it shall be escalated to [*relevant Data Protection Officers of both organisations*] who shall advise on the appropriate course of action to take;
- (b) if the matter is related to a technical element or service issue; the escalation route will be, in order;

In relation to GDS:

- (i) GDS PAAS Representatives: Mark Buckley
- (ii) GDS Director of DDaT Function and Strategy: Roxan Heaton
- (iii) GDS Director General (interim): Fiona Deans

In relation to the Tenant:

(i)

(ii)

(iii)

- (c) the representative of each Party shall work with the equivalent representative of the other Party to resolve the issue and then shall advise on the appropriate course of action to take.



### **13. GOVERNANCE AND JURISDICTION**

- 13.1. Nothing in this MOU is intended to, or shall be deemed to, establish any partnership or joint venture between the Parties, constitute either Party as the agent of the other Party, nor authorise either of the Parties to make or enter into any commitments for or on behalf of the other Party.
- 13.2. The Parties may incorporate this MOU into other agreements by reference to cover off their requirements under the GDPR under such other agreements.
- 13.3. The Parties do not intend to enter into legal relations except in respect of Schedule 1 which shall be governed by and construed in accordance with the laws of England & Wales. In the interpretation of Schedule 1 the core terms of the MOU, that is clauses 1 – 13, shall apply.

### **INCORPORATED DOCUMENTS**

The following documents shall be incorporated into this MOU.

Schedule 1: Personal Data Processing MOU between Crown body (GDS) and non-Crown body

Schedule 2: Financial Agreement

Schedule 3: Services

Schedule 4: Tenant's Responsibilities

Schedule 5: Terms of Use

Annex 1 – Details of Personal Data Exchange (template)

Annex 2 – Sub-processors

Annex 3 – Personal Data retention times

## **SCHEDULE 1**

### **PERSONAL DATA PROCESSING AGREEMENT**

This Personal Data Processing MOU (Schedule 1) is intended to comply with GDPR Article 28 and/or DPA 2018 section 59, pursuant to section 209(3) of the DPA 2018.

#### **1. REQUIREMENTS OF PARTIES TO THIS PART 1**

- 1.1. Where there is a Controller-Processor relationship, each Party shall co-operate with the other Party to complete Annex 1 prior to entering into the relationship.

#### **2. DATA PROTECTION – WHEN ONE PARTY IS CONTROLLER AND THE OTHER PARTY IS THE PROCESSOR**

- 2.1. This agreement shall apply where one Party is the Controller and the other Party is the Processor as specified in Annex 1. Subject to 2.4.1, the only Processing that the Processor is authorised to do is listed in Annex 1 by the Controller and may not be determined by the Processor.
- 2.2. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
- 2.3. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment in respect of any processing. Such assistance may, at the discretion of the Controller, include:
- (a) a systematic description of the envisaged processing operations;
  - (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
  - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
  - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 2.4. The Processor shall, in relation to any Personal Data processed in connection with its obligations under this MOU:
- 2.4.1. process that Personal Data only in accordance with Annex 1, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
  - 2.4.2. ensure that it has in place Protective Measures, which are appropriate to protect against a Personal Data Breach, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
    - 2.4.2.1. nature of the data to be protected;
    - 2.4.2.2. harm that might result from a Personal Data Breach;
    - 2.4.2.3. state of technological development; and
    - 2.4.2.4. cost of implementing any measures;
  - 2.4.3. ensure that:

- 2.4.3.1. the Processor Personnel do not process Personal Data except in accordance with this MOU (and in particular Annex 1);
- 2.4.3.2. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
  - 2.4.3.2.1. are aware of and comply with the Processor's duties under this clause;
  - 2.4.3.2.2. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
  - 2.4.3.2.3. 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 writing to do so by the Controller or as otherwise permitted by this MOU; and
  - 2.4.3.2.4. have undergone adequate training in the use, care, protection and handling of Personal Data
- 2.4.4. not transfer Personal Data outside of the EEA unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
  - 2.4.4.1. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or Chapter 5 of the DPA 2018) as determined by the Controller;
  - 2.4.4.2. the Data Subject has enforceable rights and effective legal remedies;
  - 2.4.4.3. the Processor 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 Controller in meeting its obligations); and
  - 2.4.4.4. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
- 2.4.5. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the MOU unless the Processor is required by Law to retain the Personal Data.
- 2.5. Subject to clause 2.6, the Processor [if both Parties are Processors "each Party" instead] shall notify the other Party without delay if it, in connection with Personal Data processed under this MOU:
  - 2.5.1. receives a Subject Request (or purported Subject Request);
  - 2.5.2. receives a request to rectify, block or erase any Personal Data;
  - 2.5.3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
  - 2.5.4. receives any communication from the Information Commissioner or any other regulatory authority;
  - 2.5.5. 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;

- 2.5.6. notify the other party promptly and without delay, and in any event within 48 hours, upon becoming aware of any Data Breach or circumstances that are likely to give rise to a Data Breach, providing the other Party with sufficient information and in a timescale which allows the other Party to meet any obligations to report a Data Breach under the Data Protection Laws. Such notification shall as a minimum;
- (a) Describe the nature of the Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data Records concerned;
  - (b) communicate the name and contact details of the Data Protection Officer or other relevant contact from whom more information may be obtained;
  - (c) describe the likely consequences of the Data Breach; and
  - (d) describe the measures taken or proposed to be taken to address the Data Breach,
  - (e) co-operate with the other Party and take such reasonable steps as directed by the other party to assist the investigation, mitigation and remediation of the Data Breach.
- 2.6. The Processor's obligation to notify under clause 2.5 shall include the provision of further information to the Controller in phases, as details become available.
- 2.7. Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 2.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
- 2.7.1. the Controller with full details and copies of the complaint, communication or request;
  - 2.7.2. such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Subject Request within the relevant timescales set out in the Data Protection Legislation;
  - 2.7.3. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
  - 2.7.4. assistance as requested by the Controller following any Personal Data Breach;
  - 2.7.5. assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
- 2.8. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this MOU. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
- 2.8.1. the Controller determines that the processing is not occasional;
  - 2.8.2. the Controller 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
  - 2.8.3. the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects; or
  - 2.8.4. the processing is processing to which Part 3 of the Data Protection Act 2018 applies.

- 2.9. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 2.10. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
- 2.11. Before allowing any Sub-processor to process any Personal Data related to this contract, the Processor must:
- 2.11.1. notify the Controller in writing of the intended Sub-processor and processing;
  - 2.11.2. obtain the written consent of the Controller;
  - 2.11.3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 2 such that they apply to the Sub-processor; and
  - 2.11.4. provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.
- 2.12. The Processor shall remain fully liable for all acts or omissions of any of its Sub-processor[https://docs.google.com/document/d/15xSjxbIsiov\\_noVQrl62GVAXdUIjcNMK7F1hVRDEd-g/edit?ts=5cc33457s](https://docs.google.com/document/d/15xSjxbIsiov_noVQrl62GVAXdUIjcNMK7F1hVRDEd-g/edit?ts=5cc33457s).
- 2.13. The Controller may, at any time on not less than 30 Working Days' notice, revise this clause 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).
- 2.14. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

### **3. DATA HANDLING**

#### **SERVICE DATA**

- 3.1. The Tenant is the Data Controller in relation to Service Personal Data.
- 3.2. GDS is the Processor in relation to Service Personal Data.
- 3.3. GDS will not disclose any Service Data; Service Personal Data to any outside organisation other than Sub-Processors unless permitted by the Tenant or by law.
- 3.4. The processors who may process Service Data; Service Personal Data on behalf of GOV.UK PaaS will be sourced and verified in line with GOV.UK PaaS Information Assurance and data-handling requirements in this MOU.
- 3.5. GOV.UK PaaS have the right to change Processors as they see fit to ensure GOV.UK PaaS is offering the platform outlined in the contract. The list of Processors is listed in Annex 2.
- 3.6. GDS will not retain any Service Personal Data for any longer than 2 years following termination of this MOU.

- 3.7. GDS will not retain any Service Data for longer than 2 years following the termination of this MOU.
- 3.8. GDS will process any Service Data or Service Personal Data only as set out in this MOU or on the instructions of the Tenant
- 3.9. GDS will comply with the obligations as set out under Data Protection Legislation and in particular will implement appropriate technical and organisational measures to protect any Service Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall ensure a level of security appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Service Personal Data and having regard to the nature of the Service Personal Data which is to be protected.
- 3.10. GDS will implement appropriate technical and organisational measures to protect any Service Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall ensure a level of security appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Service Data and having regard to the nature of the Service Data which is to be protected.
- 3.11. GDS will take reasonable steps to ensure that any operational GOV.UK PaaS team member will have appropriate security clearance.
- 3.12. GDS will ensure that all Personnel required to process the Service Personal Data and Service Data are informed of GDS's obligations under this contract with regard to the security and protection of Service Personal Data and Service Data and that those obligations are complied with.
- 3.13. GDS will ensure that no Personnel publish, disclose or divulge any of the Service Personal Data or Service Data to any third party unless directed in writing to do so by each of the Parties.
- 3.14. GDS will notify the Tenant within five working days if it receives a complaint or request relating to the Parties' obligations under the Data Protection Legislation.
- 3.15. If it receives a subject access request under the Data Protection Legislation, or any complaint in relation to GOV.UK PaaS, GDS will inform the complainant or requester that the Tenant is the Data Controller and ask the user to contact the Tenant.
- 3.16. GDS will not process any Service Personal Data or Service Data outside the European Economic Area without the Tenant's written permission.

### **Admin Data**

- 3.17. GDS is the Controller in relation to Admin Personal Data.
- 3.18. GDS will Process and retain Admin Personal Data only as set out in the [GOV.UK PaaS privacy notice](#).
- 3.19. GDS shall comply at all times with Data Protection Legislation and shall not perform its obligations under this contract in such a way as to cause the Tenant to breach any of its

applicable obligations under the Data Protection Legislation and any other applicable law, in particular the Human Rights Act 1998 and the common law of confidentiality.

#### **4. WARRANTY**

- 4.1. No Party to this MOU makes any warranty as to the accuracy or completeness of the Personal Data provided to another Party under this MOU.

#### **5. RECORDS**

- 5.1. Each Party shall maintain complete and accurate records and information to demonstrate its compliance with this contract and the Data Protection Legislation.
- 5.2. Each Party shall provide the other full access to the other Party's data security and privacy procedures relating to Personal Data.

#### **6. DATA BREACH LIABILITY**

- 6.1. Each Party shall ensure that its Personnel comply with Data Protection Legislation.
- 6.2. In the event that financial penalties are imposed by the Information Commissioner's Office for Data Breach, then the following will occur:
  - 6.2.1. If GDS is responsible for the relevant Data Breach, in that it is caused as a result of the team's actions or inaction of the GOV.UK PaaS team or a Processor, or systems and procedures controlled by GDS or a Sub-processor, then GDS will be responsible for the payment of these financial penalties. In this case, GDS will conduct an internal audit and engage when necessary, at its cost, an independent forensic investigator to conduct a thorough audit of any such data incident.
  - 6.2.2. If the Tenant is responsible for the relevant Data Breach, then the Tenant will be responsible for the payment of these financial penalties. GDS will provide to the Tenant and its forensic investigators and auditors, on request and at the Tenant's cost, full cooperation and access to conduct a thorough audit of any relevant data incident.
  - 6.2.3. If responsibility is unclear, then GDS and the Tenant will cooperate to investigate the Data Breach and allocate responsibility for any financial penalties as outlined above, or by agreement to split any financial penalties equally if responsibility for the Data Breach cannot be apportioned.
  - 6.2.4. If either the Tenant or GDS is the defendant in a legal action brought by a third party related to a Data Breach, then unless the Parties agree otherwise agree, the Party that is determined by the court or the ICO to be responsible for the Data Breach shall be liable for the Loss arising from such breach. Where the Parties are jointly liable the quantum will be apportioned between the Parties in accordance with the decision of the court or the ICO as the case may be.

6.2.5. A Data Breach will be grounds for immediate termination of this MOU by the Party not responsible for the Data Breach.

## **SCHEDULE 2**

### **FINANCIAL**

#### **1. Charges**

1.1 GDS will wholly pass on only those Charges it incurs for the cost of hosting the Tenant's application, including, but not limited to:

- (a) cloud infrastructure costs - such as RAM; storage and compute;
- (b) running backing services - such as databases, object storage and caches;
- (c) capacity management required to ensure Tenant application availability during maintenance and outage periods;
- (d) backup services; and
- (e) data transfer costs
- (f) administration fees

1.2 GDS will absorb the costs for the development iterations; maintenance and support of the GOV.UK PaaS platform itself.

#### **2. BILLING AND PAYMENT**

2.1 GDS and the Cabinet Office finance teams shall send Tenant an invoice for above charges on an individual basis.

## **SCHEDULE 3**

### **SERVICES**

1. GOV.UK PaaS hosts Tenant applications and Services and reduces the technical burden on Tenants to develop and maintain cloud hosting infrastructure.

2. The Service that GDS provides will be improved iteratively. It will, at a minimum, provide:

- (a) A supported platform for Tenants to host their apps/services on.
- (b) Operational support for GOV.UK PaaS that ensures technical and security issues affecting the platform are addressed without delay, including 24 hour support for critical issues. See the GOV.UK PaaS support plan for further information.

#### **Support arrangements**

3. GOV.UK PaaS will provide the Tenant with access to a ticketing system through which its admin users can request technical support. The ticketing system will enable the Tenant to



indicate the priority level of an issue raised with GOV.UK PaaS. See [GOV.UK PaaS support and response times](#) for further information.

4. General users of the Tenant's Service will not have access to support provided by GOV.UK PaaS.

## **SCHEDULE 4**

### **TENANT'S RESPONSIBILITIES**

1. The Tenant has a number of responsibilities in relation to its use of GOV.UK PaaS. These are set out below.
2. The Tenant is responsible for:
  - (a) The continued technical and user support of their application/Service.
  - (b) The security and integrity of their application/Service.
  - (c) Any technical integration work to deploy its application/Service onto GOV.UK PaaS and adhering to the guidance set out in the GOV.UK PaaS Documentation.
  - (d) Implementing suitable analytics to assist with the improvement of GOV.UK PaaS.
  - (e) Informing the GOV.UK PaaS team of any identified technical or security issues that relate to or affect GOV.UK PaaS without undue delay, and in any event no later than 48 hours after the issue is discovered. The Tenant will also assist with any investigations relating to any such issues.
  - (f) Providing contact details for key personnel to whom notifications should be sent in the event of an issue with GOV.UK PaaS.
  - (g) Not doing anything which would, or would be likely to, affect the security or integrity of GOV.UK PaaS or the systems of any Sub-processor.

## **SCHEDULE 5**

# **GOV.UK Platform as a Service (PaaS)**

## **Terms of Use**

These terms apply to our and your service's use of GOV.UK PaaS.

<https://www.cloud.service.gov.uk/terms-of-use>

## ANNEX 1

### Details of Personal Data Exchange

1.1 The contact details of the Tenant's Controller Data Protection Officer are:

[insert Tenant DPO]

1.2 The contact details of the GDS Data Processor and Data Protection Officer are:

- Cabinet Office (Government Digital Service), The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS, or [gds-privacy-office@digital.cabinet-office.gov.uk](mailto:gds-privacy-office@digital.cabinet-office.gov.uk)
- Data Protection Officer, [DPO@cabinetoffice.gov.uk](mailto:DPO@cabinetoffice.gov.uk) Cabinet Office, 70 Whitehall, London, SW1A 2AS

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.

Description	Details
Project Name and Subject Matter of the Processing	GOV.UK PaaS Public Sector employees and contractors.
Parties to the MOU	[Tenant's Organisation] Government Digital Services
Role of the Parties	Controller: [Tenant's Organisation] Processor: Government Digital Services
Duration of the processing	<ul style="list-style-type: none"><li>• For Sub-Processors - as per Annex 3 on retention periods.</li></ul>

Nature and purposes of the processing	Processing is 'for the exercise of any functions of the Crown, a Minister of the Crown or a government department'/Tenant organisation. Processing is addressed by an employment contract which the individual - or in the case of contractors, their contract entered into.
Type of Personal Data (including identifying any special category data or data relating to criminal convictions and offences)	<ul style="list-style-type: none"> <li>❖ Name</li> <li>❖ Email address</li> <li>❖ Mobile Telephone number</li> <li>❖ Organisational Role</li> <li>❖ IP address</li> </ul>
Categories of Data Subject	Public Sector employees and/or contractors in service teams using GOV.UK PaaS.
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	Secure destruction of data is automatically undertaken as per retention schedules and on contract end management with sub-processors.
Transfers to third countries or international organisations	<i>Service data and service personal data reside in the same country as where the applications and backing services are hosted.</i>
Legal Basis for Processing	<i>Public Task</i>
Special Terms	[Insert any special terms which vary the standard Terms and Conditions]

## ANNEX 2

### Sub-Processors

The Sub-Processors of GOV.UK PaaS

Organisation	Function	Data Processed	Location of data	Location of support
Amazon Web Services	Infrastructure provider for GOV.UK PaaS	Service Data; Service Personal Data; Admin Personal Data	EEA: Primarily Dublin & London	Primarily EEA plus other geographical locations for out of hours support
Aiven	Elasticsearch database SaaS provider	Service data	London and Dublin	Finland
Zendesk	Customer Support helpdesk	Personal Data; Service Personal Data	US	UK/US
Logit	Logging storage and analytic solution for GOV.UK PaaS.	Service Data; Admin Personal Data	UK	Manchester, UK

### Annex 3 - Personal Data Retention Times

Organisation	Personal Data retention time (where the Tenant is the data controller)	Admin Personal Data retention time (where GOV.UK PaaS is the data controller)
GOV.UK PaaS	35 days	1 - 2 years
Amazon Web Services	35 days	35 days
Aiven	Information is available for 7, 14 or 30 days after the instance has been deleted in the form of a backup.	35 days
Zendesk	n/a	1 - 2 years
Logit	30 days	on account

**This Memorandum of Understanding is agreed:**

**For and on behalf of THE MINISTER FOR THE CABINET OFFICE**

---

Name:

Position:

Date:

**For and on behalf of the [Insert Tenant Body]**

---

Name:

Position:

Date: