# SHORT FORM CONTRACT FOR THE SUPPLY OF GOODS AND/OR SERVICES

## I. Index

## II. Cover Letter (Not Used)

## III. Order Form

| | | | |
|---|---|---|---|
| **1. Contract Reference** | SR2497129644 | | |
| **2. Buyer** | HMRC, (100 Parliament Street Westminster London SW1A 2BQ). In entering into this Contract, the Buyer is acting as part of the Crown and the Supplier shall be treated as contracting with the Crown as a whole. | | |
| **3. Supplier** | GitLab UK Limited Suite 4, 7TH Floor 50 Broadway London, SW1H 0DB, United Kingdom | | |
| **4. The Contract** | This Contract between the Buyer and the Supplier is for the supply of Deliverables.<br>The Supplier shall supply the Deliverables described below on the terms set out in this Order Form and the attached contract conditions ("**Conditions**") and Annexes.<br>Unless the context otherwise requires, capitalised expressions used in this Order Form have the same meanings as in the Conditions. | | |
| **5. Deliverables** | **Goods** | None | |
| | **Services** | GitLab's Dedicated offering:<br>- Special Terms 1 – GitLab Subscription Agreement - Specification<br>Professional Services provided by GitLab:<br>● in Special Terms 2 – Work Description | |
| **6. Specification** | The specification of the Deliverables is as set out:<br>● in Annex 2 – Specification | | |
| **7. Start Date** | 29/09/2025 | | |

| | |
|---|---|
| **8. Expiry Date** | 28/09/2028 |

| | |
|---|---|
| **9. Extension Period** | Not applicable |
| **10. Buyer Cause** | Any Material Breach of the obligations of the Buyer or any other default, act, omission, negligence or statement of the Buyer, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Buyer is liable to the Supplier. |
| **11. Optional Intellectual Property Rights ("IPR") Clauses** | Clause 10 shall be deleted and replaced with the clauses set out in Part B of Annex 5 – Optional IPR Clauses |
| **12. Charges** | The Charges for the Deliverables shall be as set out<br>● in Annex 3 – Charges |

| | |
|---|---|
| **13. Payment** | If the Buyer purchases via the AWS marketplace, payment terms and invoicing shall be as agreed between buyer and AWS.<br><br>Payment of valid and undisputed invoices will be made within 30 days of receipt of the invoice or, if later, the date by which the payment falls due in accordance with the invoice, which must be submitted promptly by the Supplier.<br><br>All invoices must be sent, quoting a valid Purchase Order Number (PO Number) and any other relevant details including the minimum required information set out in Section 68(9) of the Procurement Act 2023, via the SAP Ariba system.<br><br>Within 10 Working Days of receipt of your countersigned copy of this Order Form, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice.<br><br>To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, item number (if applicable) and the details (name, email, and telephone number) of your Buyer contact (i.e. Buyer Authorised Representative). Non-compliant invoices may be sent back to you, which may lead to a delay in payment.<br><br>Payments will be made via the SAP Ariba System.<br><br>If you have a query regarding an outstanding payment please contact our Accounts Payable team by email to: [redacted] between 09:00-17:00 Monday to Friday. |

| | |
|---|---|
| **14. Data Protection Liability Cap** | In accordance with clause 12.6 of the Conditions, the Supplier's total aggregate liability under clause 14.5.4 of the Conditions is no more than the Data Protection Liability Cap, being no more, in aggregate, than 125% of the Charges paid or payable to the Supplier in the one-year period preceding the first incident out of which the liability arose. |
| **15. Progress Meetings and Progress Reports** | The Supplier shall attend Quarterly Business Review Meetings with the Buyer once per quarter of each Contract Year. |
| **16. Buyer Authorised Representative (s)** | For general liaison your contact will continue to be<br>[redacted] |

| | |
|---|---|
| **17. Supplier Authorised Representative (s)** | For general liaison (no signatory authority) your contact will continue to be [redacted] or, in their absence, [redacted] |
| **18. Address for notices** | In accordance with clause 26.1, all notices under the Contract shall be in writing and will be served by e-mail unless it is not practicable to do so.<br>[redacted] GitLab Legal Department<br>Attention: [redacted] [redacted]<br>Address: [redacted] |
| **19. Key Staff** | Not Applicable |
| **20. Procedures and Policies** | For the purposes of the Contract the Supplier shall perform background checks of its staff as set out at https://handbook.gitlab.com/handbook/peoplegroup/contracts-probation-periods/ and subject to Section 3 of Appendix 1 of Schedule 16. |
| **21. Optional Security Requirements** | The following Schedule shall apply to this Contract: Schedule 16 – Security Buyer-Led Assurance |
| **22. Special Terms** | Special Term 1 - GitLab Subscription Agreement |
| | Special Term 2 - Description of Work (Professional Services) |

| | |
|---|---|
| | Special Term 3 - The parties agree that the IDTA, as annexed hereto as Annex 6, shall apply to all restricted transfers of personal data under this Agreement. In the event of any conflict between this Agreement and the IDTA, the terms of the IDTA shall prevail in respect of such transfers. |
| **23. Incorporated Terms** | The following documents are incorporated into the Contract. If there is any conflict, the following order of precedence applies:<br>(a) This Order Form<br>(b) Any Special Terms (see row 22 (Special Terms) in this Order Form)<br>(c) Conditions (as they may be amended by Annex 5 – Optional IPR Clauses (Optional))<br>(d) The following Annexes in equal order of precedence:<br>i. Annex 1 – Processing Personal Data<br>ii. Annex 2 – Specification<br>iii. Annex 3 – Charges<br>iv. Schedule 16 – Security Buyer-Led Assurance Schedule 1 (Performance Levels)<br>v. Schedule 2 AUTHORITY'S MANDATORY TERMS |

| Signed for and on behalf of the Supplier | Signed for and on behalf of the Buyer acting on behalf of the Crown |
|---|---|
| Name: [redacted] | Name: [redacted] |
| Date: [redacted] | Date: [redacted] |
| Signature: [redacted] | Signature: [redacted] |

## IV. Short form Terms ("Conditions")

1. Definitions used in the Contract

1.1 In this Contract, unless the context otherwise requires, the following words shall have the following meanings:

| | | |
|---|---|---|
| **1** | **"Affiliates"** | 1 in relation to a body corporate, any other entity which directly or indirectly Controls (in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly), is Controlled by, or is under direct or indirect common Control of that body corporate from time to time; |
| **2** | **"Audit"** | 1 the Buyer's right to:<br>(a) verify the accuracy of the Charges and any other amounts payable by the Buyer under the Contract (including variations to them in accordance with the Contract);<br>(b) verify the costs of the Supplier submitted for reimbursement in connection with the provision of professional services in accordance with the Description of Work;<br>(c) verify the Supplier's compliance with the applicable Law;<br>(d) identify breach of clauses 4 to 33 (inclusive), impropriety or accounting mistakes or any breach of security;<br>(e) obtain such information as is necessary to fulfil the Buyer's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General;<br>(f) carry out the Buyer's internal and statutory audits and to prepare, examine and/or certify the Buyer's annual and interim reports and accounts;<br>(g) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Buyer has used its resources; |
| **3** | **"Beneficiary"** | 1 a Party having (or claiming to have) the benefit of an indemnity under this Contract; |
| **4** | **"Buyer Cause"** | 1 has the meaning given to it in the Order Form; |

| | |
|---|---|
| **5 "Buyer"** | 1 the person named as Buyer in the Order Form. Where the Buyer is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole; |
| **6 "Charges"** | 1 the charges for the Deliverables as specified in the Order Form; |
| **7 "Claim"** | 1 any claim which it appears that a Party is, or may become, entitled to indemnification under this Contract; |
| **8 "Conditions"** | 1 these short form terms and conditions of contract; |
| **9 "Confidential Information"** | 1 all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (a) is known by the receiving Party to be confidential;<br>(b) is marked as or stated to be confidential; or<br>(c) ought reasonably to be considered by the receiving Party to be confidential; |
| **10 "Conflict of Interest"** | 1 a material conflict between the financial, professional or personal interests of the Supplier or the Supplier Staff and the duties owed to the Buyer under the Contract, in the reasonable opinion of the Buyer, acting in good faith and as would be held by a reasonable person in the Buyer's position; and that directly and adversely affects the performance of the Supplier's obligations under this Contract or the Supplier's or Buyer's ability to comply with applicable laws; |
| **11 "Contract"** | 1 the contract between the Buyer and the Supplier which is created by the Supplier's counter signing the Order Form and includes the cover letter (if used), Order Form, these Conditions and the Annexes; |
| 12 **"Contract Year"** | (a) a period of 12 months commencing on the Start Date; and<br>(b) thereafter a period of 12 months commencing on each anniversary of the Start Date,<br>2 with the final Contract Year ending on the expiry or termination of the Term; |

| | |
|---|---|
| **13 "Controller"** | 1 has the meaning given to it in the UK GDPR or the EU GDPR as the context requires; |
| **14 "Crown Body"** | 1 the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the Welsh Government), including, but not limited to, government ministers and |

| | |
|---|---|
| | government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf; |
| **15 "Data Loss Event"** | 1 any event that results or is likely to result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or likely loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach, provided that Supplier shall not be liable for any Data Loss event caused by the Buyer's personnel, or circumstances beyond Processor's reasonable control; |
| **16 "Data Protection Impact Assessment"** | 1 an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data; |
| **17 "Data Protection Legislation"** | (a) the UK GDPR, (b) the DPA 2018;<br>(c) all applicable Law about the processing of personal data and privacy and guidance issued by the Information Commissioner and other regulatory authority; and<br>(d) (to the extent that it applies) the EU GDPR (and in the event of conflict, the UK GDPR shall apply); |
| **18 "Data Protection Liability Cap"** | 1 has the meaning given to it in row 14 of the Order Form; |
| **19 "Data Protection Officer"** | 1 has the meaning given to it in the UK GDPR or the EU GDPR as the context requires; |
| **20 "Data Subject Access Request"** | 1 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; |

| | |
|---|---|
| **21 "Data Subject"** | 1 has the meaning given to it in the UK GDPR or the EU GDPR as the context requires; |
| **22 "Deliver"** | 1 hand over of the Deliverables to the Buyer at the address and on the date specified in the Order Form, which shall include unloading and stacking and any other specific arrangements agreed in accordance with clause 4.2. "Delivered" and "Delivery" shall be construed accordingly; Not applicable |
| **23 "Deliverables"** | 1 the Goods, Services, and/or software to be supplied under the Contract as set out in the Order Form; |

| | |
|---|---|
| **24 "Developed System"** | 1 the software or system that the Supplier is required to develop under this Contract; Not applicable |
| **25 "DPA 2018"** | 1 the Data Protection Act 2018; |
| **26 "EU GDPR"** | 1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law; |
| **27 "Existing IPR"** | 1 any and all intellectual property rights that are owned by or licensed to either Party and which have been developed independently of the Contract (whether prior to the date of the Contract or otherwise); |
| **28 "Expiry Date"** | 1 the date for expiry of the Contract as set out in the Order Form; |
| **29 "FOIA"** | 1 the Freedom of Information Act 2000 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation; |
| **30 "Force Majeure Event"** | 1 (a) any event, circumstance, matter or cause affecting the non-monetary ıance by either the Buyer or the Supplier of its obligations arising from:<br>acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Party seeking to claim relief in respect of a Force Majeure Event (the **"Affected Party"**) which prevent or materially delay the Affected Party from performing its obligations under the Contract;<br>(b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; |

| | |
|---|---|
| | (c) acts of a Crown Body (excluding the Buyer), or regulatory bodies;<br>(d) fire, flood or any disaster; or<br>(e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available<br>2 but excluding:<br>(a) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them);<br>(b) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and<br>(c) any failure of delay caused by a lack of funds, |

| | |
|---|---|
| | 3 and which is not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party; |
| **31 "Good Industry Practice"** | 1 standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector; |
| **32 "Goods"** | 1 the goods to be supplied by the Supplier to the Buyer under the Contract; |

| | |
|---|---|
| **33 "Government Data"** | any:<br>(a) data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media;<br>(b) Personal Data for which the Buyer is a, or the, Data Controller; or<br>(c) any meta-data relating to categories of data referred to in (a) or (b)<br>that:<br>(i) is supplied to the Supplier by or on behalf of the Buyer; and/or<br>(ii) that the Supplier is required to generate, Process, Handle, store or transmit under this Contract; |
| **34 "IDTA"** | means the International Data Transfer Agreement issued by the UK Information Commissioner's Office, annexed to this Agreement as Annex 6. |
| **35 "Indemnifier"** | 1 a Party from whom an indemnity is sought under this Contract; |
| **36 "Independent Controller"** | 1 a party which is Controller of the same Personal Data as the other Party and there is no element of joint control with regards to that Personal Data; |
| **37 "Information Commissioner"** | 1 the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies; |
| **38 "Insolvency Event"** | 1 in respect of a person: |

| | |
|---|---|
| | (a) if that person is insolvent;<br>(b) where that person is a company, LLP or a partnership, if an order is made or a resolution is passed for the winding up of the person (other than voluntarily for the purpose of solvent amalgamation or reconstruction);<br>(c) if an administrator or administrative receiver is appointed in respect of the whole or any part of the person's assets or business;<br>(d) if the person makes any composition with its creditors; or<br>(e) takes or suffers any similar or analogous action to any of the actions detailed in this definition as a result of debt in any jurisdiction; |
| **39 "IP Completion Day"** | 1 has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020; Not applicable |
| **40 "IR35"** | 1 Chapter 8 and Chapter 10 of Part 2 of Income Tax (Earnings and Pensions) Act 2003 and the Social Security Contributions (Intermediaries) Regulations 2000; |
| **41 "Joint Controller Agreement"** | 1 the agreement (if any) entered into between the Buyer and the Supplier substantially in the form set out in Part B Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data; Not Applicable |
| **42 "Joint Controllers"** | 1 where two or more Controllers jointly determine the purposes and means of processing; Not Applicable |
| **43 "Key Staff"** | 1 any persons specified as such in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier; Not Applicable |
| **44 "Law"** | 1 any law, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, right within the meaning of the European Union (Withdrawal) Act 2018 as amended by European Union (Withdrawal Agreement) Act 2020, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply; |
| **45 "Material Breach"** | 1 a single serious breach or a number of breaches or repeated breaches (whether of the same or different obligations and regardless of whether such breaches are remedied) that substantially deprives the innocent Party of the benefit intended to be obtained under the Contract or goes to the essence of the Contract |

| | |
|---|---|
| **46 "National Insurance"** | 1 contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004); |
| **47 "New IPR Items"** | 1 a deliverable, document, product or other item within which New IPR subsists; Not Applicable – No New IPR Items is in scope under this Contract |
| **48 "New IPR"** | 1 all and intellectual property rights in any materials created or developed by or on behalf of the Supplier pursuant to the Contract but shall not include the Supplier's Existing IPR; Not Applicable – No New IPR Items is in scope under this Contract |
| **49 "Open Licence"** | 1 any material that is published for use, with rights to access and modify, by any person for free, under a generally recognised open licence including Open Government Licence as set out at http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ as updated from time to time and the Open Standards Principles documented at https://www.gov.uk/government/publications/open-standards-principles/openstandards-principles as updated from time to time; |
| **50 "Order Form"** | 1 the order form signed by the Buyer and the Supplier printed above these Conditions; |
| **51 "Party"** | 1 the Supplier or the Buyer (as appropriate) and "Parties" shall mean both of them; |
| **52 "Personal Data Breach"** | 1 has the meaning given to it in the UK GDPR or the EU GDPR as the context requires and includes any breach of Data Protection Legislation relevant to Personal Data processed pursuant to the Contract; |
| **53 "Personal Data"** | 1 has the meaning given to it in the UK GDPR or the EU GDPR as the context requires; |

| | |
|---|---|
| **54 "Prescribed Person"** | 1 a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-ofprescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-andbodies as updated from time to time; |
| **55 "Processor Personnel"** | 1 all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Sub-processor engaged in the performance of its obligations under the Contract; |

| | |
|---|---|
| **56 "Processor"** | 1 has the meaning given to it in the UK GDPR or the EU GDPR as the context requires; |
| **57 "Protective Measures"** | 1 technical and organisational measures which must take account of:<br>(a) the nature of the data to be protected;<br>(b) harm that might result from Data Loss Event;<br>(c) state of technological development;<br>(d) the cost of implementing any measures;<br>2 including 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, including those outlined in Annex 1 *(Processing Personal Data)* and Schedule 16 – Security Buyer-Led Assurance; |
| **58 "Purchase Order Number" or "PO Number"** | 1 the Buyer's unique number relating to the order for Deliverables to be supplied by the Supplier to the Buyer in accordance with the Contract; |

| | |
|---|---|
| **59 "Rectification Plan"** | 1 the Supplier's plan (or revised plan) to rectify its Material Breach which shall include:<br>(a) full details of the Material Breach that has occurred, including a root cause analysis;<br>(b) the actual or anticipated effect of the Material Breach; and<br>(c) the steps which the Supplier proposes to take to rectify the Material Breach (if applicable) and to prevent such Material Breach from recurring, including timescales for such steps and for the rectification of the Material Breach (where applicable); |
| **60 "Regulations"** | 1 the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires) as amended from time to time; |
| **61 "Request For Information"** | 1 has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term "**request**" shall apply); |
| **62 "Security Requirements"** | 1 the security requirements set out in the Order Form or in Schedule 16 – Security Buyer-Led Assurance; |

| | |
|---|---|
| **63 "Services"** | 1 the services to be supplied by the Supplier to the Buyer under the Contract; |
| **64 "Specification"** | 1 the specification for the Deliverables to be supplied by the Supplier to the Buyer (including as to quantity, description and quality) as specified in the Order Form; |
| **65 "Start Date"** | 1 the start date of the Contract set out in the Order Form; |

| | |
|---|---|
| **66 "Sub-Contract"** | 1 any contract or agreement (or proposed contract or agreement), other than the Contract, pursuant to which a third party: (a) provides the Deliverables (or any part of them);<br>(b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or<br>(c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them); |
| **67 "Subcontractor"** | 1 any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person; |
| **68 "Subprocessor"** | 1 any third party appointed to process Personal Data on behalf of the Processor related to the Contract; |
| **69 "Supplier Staff"** | 1 any individual engaged, directly or indirectly, or employed by the Supplier or any Subcontractor, in the management or performance of the Supplier's obligations under this Contract; |
| **70 "Supplier"** | 1 the person named as Supplier in the Order Form; |
| **71 "Supply Chain Intermediary"** | 1 any entity (including any company or partnership) in an arrangement with a Worker, where the Worker performs or is under an obligation personally to perform, services for the Buyer; Not Applicable – No Supply Chain Intermediary |
| **72 "Term"** | 1 the period from the Start Date to the Expiry Date as such period may be extended in accordance with clause 11.2 or terminated in accordance with the Contract; |
| **73 "Third Party IPR"** | 1 intellectual property rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables; |

| | |
|---|---|
| **74 "Transparency Information"** | (a) any information which must be published pursuant to guidance issued by His Majesty's Government, from time to time;<br>(b) any information or notices required to be published by the Procurement Act 2023, any Regulations published under it, and any PPNs, subject to any exemptions set out in sections 94 and 99 of the Procurement Act 2023, which shall be determined by the Buyer, taking into consideration any information which is Confidential Information; and<br>(c) any information about the Contract, including the content of the Contract, and any changes to this Contract agreed from time to time, as well as any information relating to the Deliverables and performance pursuant to the Contract required to be disclosed under FOIA or the Environmental Information Regulations 2004, subject to any exemptions, which shall be determined by the Buyer, taking into consideration any information which is Confidential Information; |
| **75 "US Data Privacy Framework"** | 1 as applicable: (a) the UK Extension to the EU-US Data Privacy Framework; and/or (b) the EU-US Data Privacy Framework; |
| **76 "UK GDPR"** | 1 has the meaning as set out in section 3(10) of the DPA 2018, supplemented by section 205(4); |
| **77 "VAT"** | 1 value added tax in accordance with the provisions of the Value Added Tax Act 1994; |
| **78 "Worker"** | 1 any individual that personally performs, or is under an obligation personally to perform services for the Buyer; Not Applicable |
| **79 "Working Day"** | 1 a day (other than a Saturday or Sunday) on which banks are open for business in the City of London. |

2. Understanding the Contract

2.1 In the Contract, unless the context otherwise requires:

2.1.1 references to numbered clauses are references to the relevant clause in these Conditions;

2.1.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;

2.1.3 references to "writing" include printing, display on a screen and electronic transmission and other modes of representing or reproducing words in a visible form;

2.1.4 a reference to a Law includes a reference to that Law as modified, amended, extended, consolidated, replaced or re-enacted (including as a consequence of the Retained EU Law (Revocation and Reform) Act 2023) from time to time before or after the date of this Contract and any prior or subsequent legislation under it;

2.1.5 the word "including", "for example" and similar words shall be understood as if they were immediately followed by the words "without limitation";

2.1.6 any reference which, immediately before IP Completion Day (or such later date when relevant EU law ceases to have effect pursuant to section 1A of the European Union (Withdrawal) Act 2018), is a reference to (as it has effect from time to time) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement (**"EU References"**) 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 IP Completion 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

2.1.7 a reference to a document (including this Contract) is to that document as varied, amended, novated, ratified or replaced from time to time.

3. How the Contract works

3.1 The Order Form is an offer by the Buyer to purchase the Deliverables subject to and in accordance with the terms and conditions of the Contract.

3.2 The Supplier is deemed to accept the offer in the Order Form when the Buyer receives a copy of the Order Form signed by the Supplier.

3.3 Intentionally omitted.

4. What needs to be delivered

**4.1 All Deliverables**

4.1.1 The Supplier must provide Deliverables:

4.1.1.1 in accordance with the Specification, and the Contract;

4.1.1.2 using reasonable skill and care;

4.1.1.3 using Good Industry Practice;

4.1.1.4 using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract;

4.1.1.5 on the dates agreed; and

4.1.1.6 that comply with all Law applicable to the Supplier and the provision of the Deliverables by Supplier.

4.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days (or longer where the Supplier offers a longer warranty period to its Buyers).

**4.2 Goods clauses (Not Applicable)**

4.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.

4.2.2 The Supplier transfers ownership of the Goods on completion of Delivery or payment for those Goods, whichever is earlier.

4.2.3 Risk in the Goods transfers to the Buyer on Delivery, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

4.2.4 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

4.2.5 The Supplier must Deliver the Goods on the date and to the location specified in the Order Form, during the Buyer's working hours (unless otherwise specified in the Order Form).

4.2.6 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

4.2.7 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

4.2.8 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

4.2.9 The Supplier will notify the Buyer of any request that Goods are returned to it or the manufacturer after the discovery of safety issues or defects that might endanger health or hinder performance and shall indemnify the Buyer against the costs arising as a result of any such request.

4.2.10 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days' notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable endeavours to minimise these costs.

4.2.11 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with clause 4.2. If the Supplier doesn't do this it will pay the Buyer's costs including repair or re-supply by a third party.

4.2.12 The Buyer will not be liable for any actions, claims, costs or expenses incurred by the Supplier or any third party during Delivery of the Goods unless and to the extent that it is caused by negligence or other wrongful act of the Buyer or its servant or agent. If the Buyer suffers or incurs any damage or injury (whether fatal or otherwise) occurring in the course of Delivery or installation then the Supplier shall indemnify the Buyer from any losses, charges, costs or expenses which arise as a result of or in connection with such damage or injury where it is attributable to any act or omission of the Supplier or any of its Subcontractors or Supplier Staff.

**4.3 Professional Services clauses**

4.3.1 Late Delivery of the Services will be a default of the Work Description.

4.3.2 The Supplier must reasonably co-operate with the Buyer and third party suppliers on all aspects connected with the delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions including the Security Requirements (where any such requirements have been provided and where such requirements apply due to access to Buyer systems or premises).

4.3.3 The Buyer must provide the Supplier with reasonable access to its premises at reasonable times for the purpose of supplying the Services

4.3.4 The Supplier must at its own risk and expense provide all equipment required to deliver the Services. Any equipment provided by the Buyer to the Supplier for supplying the Services remains the property of the Buyer and is to be returned to the Buyer on expiry or termination of the Contract.

4.3.5 The Supplier must allocate sufficient resources and appropriate expertise to the Contract.

4.3.6 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.

4.3.7 On completion of the Services, the Supplier is responsible for leaving the Buyer's premises in a clean, safe and tidy condition and making good any damage that it has caused to the Buyer's premises or property, other than fair wear and tear.

4.3.8 The Supplier must ensure all Services, and anything used to deliver the Services, are of industry standard quality.

4.3.9 The Buyer is entitled to withhold payment in good faith and acting reasonably for partially or undelivered Services, in proportion to the extent of non-delivery, but doing so does not stop it from using its other rights under the Contract.

5. Pricing and payments

5.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the charges in the Order Form.

5.2 All Charges:

5.2.1 exclude VAT, which is payable on provision of a valid VAT invoice; and

5.2.2 include all costs and expenses connected with the supply of Deliverables.

5.3 The Buyer must pay the Supplier the charges:

5.3.1 within 30 days beginning with the day on which an invoice is received by the Buyer in respect of the sum, or

5.3.2 if later, the day by which the payment falls due in accordance with the invoice,

subject to the invoice being verified as valid and not reasonably disputed in good faith.

5.4 A Supplier invoice is only valid if it:

5.4.1 includes the minimum required information set out in Section 88(7) of the Procurement Act 2023;

5.4.2 includes all appropriate references including the Purchase Order Number and other details reasonably requested by the Buyer and communicated to the Supplier in advance in writing; and

5.4.3 includes a detailed breakdown of Deliverables which have been delivered.

5.5 If there is a reasonable, good faith dispute between the Parties as to the amount invoiced, the Buyer shall pay the undisputed amount. The Supplier shall not suspend the provision of the Deliverables unless the Supplier is entitled to terminate the Contract for a failure to pay undisputed sums in accordance with clause 11.6. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 35.

5.6 Intentionally omitted .

5.7 The Supplier must ensure that all Subcontractors are paid, in full:

5.7.1 within 30 days beginning with the day on which an invoice is received by the Buyer in respect of the sum; or

5.7.2 if later, the date by which the payment falls due in accordance with the invoice,

subject to the invoice being verified as valid and undisputed.

5.8 If the invoice is not paid in accordance with the timescales in clause 5.7, the Buyer can publish the details of the late payment or non-payment.

5.9 Where any invoice does not conform to the Buyer's requirements set out in clause 5.4, or the Buyer disputes the invoice, the Buyer shall notify the Supplier without undue delay and the Supplier shall promptly issue a replacement invoice which shall comply with such requirements.

6. The Buyer's obligations to the Supplier

6.1 If Supplier fails to comply with the Contract as a result of a Buyer Cause:

6.1.1 the Buyer cannot terminate the Contract under clause 11;

6.1.2 the Supplier is entitled to reasonable and proven additional expenses and to relief from liability under this Contract;

6.1.3 the Supplier is entitled to additional time needed to deliver the Deliverables; and

6.1.4 Intentionally omitted.

6.2 With respect to Clause 6.1 the Supplier shall take reasonable efforts to:

6.2.1 give notice to the Buyer within 10 Working Days of becoming aware;

6.2.2 demonstrate that the failure only happened because of the Buyer Cause; and

6.2.3 mitigate the impact of the Buyer Cause.

7. Record keeping and reporting

7.1 The Supplier must ensure that suitably qualified representatives attend progress

meetings with the Buyer, upon reasonable notice by the Buyer and at a mutually agreed time, and provide progress reports when specified in the Order Form, provided that the Buyer shall provide the reasonably necessary reporting requirements at least thirty (30) days in advance.

7.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract in accordance with its Record Retention Policy at https://handbook.gitlab.com/handbook/legal/record-retention-policy/ and in accordance with the UK GDPR or the EU GDPR as the context requires.

7.3 The Supplier must, no more than once per annum, provide an auditor appointed by the Buyer information to verify Supplier's compliance with the Contract and provide copies for the Audit.

7.4 The Buyer or an auditor can Audit the Supplier in accordance with the terms set out in this Contract.

7.5 During an Audit, the Supplier must provide information reasonably requested and to the extent relevant to the provision of the Services, to the auditor and reasonable co-operation at their request.

7.6 The Parties will bear their own costs when an Audit is undertaken.

7.7 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

7.7.1 tell the Buyer and give reasons;

7.7.2 propose corrective action; and

7.7.3 provide a deadline for completing the corrective action.

7.8 If the Buyer, acting reasonably, and based on objective evidence which it shall specify in writing is concerned as to the financial stability of the Supplier such that it has substantial likelihood of impacting on the continued performance of the Contract then the Buyer may:

7.8.1 require that the Supplier provide to the Buyer (for its approval) a plan within 30 days setting out how the Supplier will ensure continued performance of the Contract and the Supplier will make changes to such plan as reasonably required by the Buyer and once it is agreed then the Supplier shall act in accordance with such plan and report to the Buyer no more than monthly, provided all such information remains strictly confidential.

7.8.2 if the Supplier deliberately or negligently fails to provide a plan or fails to implement agreed measures included in a plan within the timeframes specified therein, or provide updates on progress with the plan, terminate the Contract, provided that such failure constitutes a Material Breach, in which case the consequences of termination in clause 11.5.1 shall apply.

7.9 If there is a Material Breach by the Supplier the Buyer may request that the Supplier provide a Rectification Plan within 10 Working Days of the Buyer's request alongside any additional applicable documentation that the Buyer reasonably requires. Once such Rectification Plan is agreed between the Parties (without the Buyer limiting its rights) the Supplier must immediately start work on the actions in the Rectification Plan at its own cost.

7.10 At the end of each Contract Year, at its own expense and upon the Buyer's request, the Supplier will provide an attestation to the Buyer confirming its compliance with clause 5.7, such report to be signed by the Supplier's Authorised Representative as being accurate and not misleading.

8. Supplier Staff

8.1 The Supplier Staff involved in the performance of the Contract must:

8.1.1 be appropriately trained and qualified;

8.1.2 be vetted in accordance with the Supplier's staff vetting procedures and subject to Section 3 of Appendix 1 of Schedule 16 *(Security Requirements)* (if used); and

8.1.3 comply with all reasonable conduct requirements when on the Buyer's premises.

8.2 Where the Buyer reasonably decides in good faith that one of the Supplier's Staff directly involved in providing professional services to the Buyer under this Contract isn't suitable to work on the Contract due to documented material performance deficiencies, professional misconduct, or material breach of confidentiality obligations, and provides written notice with specific reasons, the Supplier must use reasonable efforts to replace them with a suitably qualified alternative within a reasonable timeframe not exceeding 60 days, subject to availability of qualified personnel. This provision shall not apply to administrative, support or any other Staff not directly engaged in professional service delivery.

8.3 The Supplier must provide a list of Supplier Staff needing to access the Buyer's premises and say why access is required.

8.4 The Supplier indemnifies the Buyer against all claims brought by any person employed or engaged by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8.5 The Buyer indemnifies the Supplier against all claims brought by any person employed or engaged by the Buyer caused by an act or omission of the Buyer or any of the Buyer's employees, agents, consultants and contractors.

8.6 The Supplier shall use those persons nominated (if any) as Key Staff in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier to provide the Deliverables and shall not remove or replace any of them unless:

8.6.1 requested to do so by the Buyer or the Buyer approves such removal or replacement (not to be unreasonably withheld or delayed);

8.6.2 the person concerned resigns, retires or dies or is on parental or longterm sick leave; or

8.6.3 the person's employment or contractual arrangement with the Supplier or any Subcontractor is terminated for material breach of contract by the employee.

8.7 The Supplier shall ensure that no person who discloses that they have a conviction

that is relevant to the nature of the Contract, relevant to the work of the Buyer, or is of a type otherwise advised by the Buyer (each such conviction a "**Relevant Conviction**"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a disclosure and barring service check or otherwise) is employed or engaged in the provision of any part of the Deliverables.

9. Rights and protection

9.1 The Supplier undertakes and confirms that:

9.1.1 it has full capacity and authority to enter into and to perform the Contract;

9.1.2 the Contract is entered into by its authorised representative;

9.1.3 it is a legally valid and existing organisation incorporated in the place it was formed;

9.1.4 there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its affiliates that might affect its ability to perform the Contract;

9.1.5 all necessary rights, authorisations, licences and consents (including in relation to IPRs) are in place to enable the Supplier to perform its obligations under the Contract and the Buyer to receive the Deliverables;

9.1.6 it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform the Contract; and

9.1.7 it is not impacted by an Insolvency Event.

9.2 The undertakings in clause 9.1 are repeated each time the Supplier provides Deliverables under the Contract.

9.3 The Supplier shall be liable to the Buyer fort each of the following:

9.3.1 wilful misconduct of the Supplier, any of its Subcontractor and/or Supplier Staff that impacts the Contract; and

9.3.2 non-payment by the Supplier of any tax or National Insurance.

9.4 If the Supplier becomes aware of a representation or warranty made in relation to the Contract that becomes untrue or misleading, it must immediately notify the Buyer.

9.5 Intentionally omitted.

10. Intellectual Property Rights ("IPRs") **Not Applicable**

10.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable, sublicensable worldwide licence to use, copy and adapt the Supplier's Existing IPR to enable the Buyer and its sub-licensees to both:

10.1.1 receive and use the Deliverables; and

10.1.2 use the New IPR.

The termination or expiry of the Contract does not terminate any licence granted under this clause 10.

10.2 Any New IPR created under the Contract is owned by the Buyer. The Buyer gives the Supplier a royalty-free, non-exclusive, non-transferable licence to use, copy, and adapt any Existing IPRs and the New IPR which the Supplier reasonably requires for the purpose of fulfilling its obligations during the Term and commercially exploiting the New IPR developed under the Contract. This licence is sub-licensable to a Subcontractor for the purpose of enabling the Supplier to fulfil its obligations under the Contract, and in that case the Subcontractor must enter into a confidentiality undertaking with the Supplier on the same terms as set out in clause 15 (What you must keep confidential).

10.3 Unless otherwise agreed in writing, the Supplier and the Buyer will record any New IPR and keep this record updated throughout the Term.

10.4 Where a Party acquires ownership of intellectual property rights incorrectly under this Contract, it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

10.5 Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in this clause 10 or otherwise agreed in writing.

10.6 If any claim is made against the Buyer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Deliverables (an "**IPR Claim**"), then the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result of the IPR Claim.

10.7 If an IPR Claim is made or anticipated, the Supplier must at its own option and expense, either:

10.7.1 obtain for the Buyer the rights in clause 10.1 without infringing any thirdparty intellectual property rights; and

10.7.2 replace or modify the relevant item with substitutes that don't infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.

10.7.3 If the Supplier is not able to resolve the IPR Claim to the Buyer's reasonable satisfaction within a reasonable time, the Buyer may give written notice that it terminates the Contract from the date set out in the notice, or where no date is given in the notice, the date of the notice. On termination, the consequences of termination in clause 11.5.1 shall apply.

10.8 The Supplier shall not use in the Delivery of the Deliverables any Third Party IPR unless:

10.8.1 the Buyer gives its approval to do so; and

10.8.2 one of the following conditions applies:

10.8.2.1 the owner or an authorised licensor of the relevant Third Party IPR has granted the Buyer a direct licence that provides the Buyer with the rights in clause 10.1; or

10.8.2.2 if the Supplier cannot, after commercially reasonable endeavours, obtain for the Buyer a direct licence to the Third Party IPR as set out in clause 10.8.2.1:

(a) the Supplier provides the Buyer with details of the licence terms it can obtain and the identity of those licensors;

(b) the Buyer agrees to those licence terms; and

(c) the owner or authorised licensor of the Third Party IPR grants a direct licence to the Buyer on those terms; or

10.8.2.3 the Buyer approves in writing, with reference to the acts authorised and the specific intellectual property rights involved.

10.9 In spite of any other provisions of the Contract and for the avoidance of doubt, award of this Contract by the Buyer and the ordering of any Deliverable under it, does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977, Section 12 of the Registered Designs Act 1949 or Sections 240 – 243 of the Copyright, Designs and Patents Act 1988.

11. Ending the contract

11.1 The Contract takes effect on the Start Date and ends on the earlier of the Expiry Date or termination of the Contract, or earlier if required by Law.

11.2 The Buyer can extend the Contract where set out in the Order Form in accordance with the terms in the Order Form. (Not Applicable)

11.3 **Ending the Contract without a reason**

Neither Party has the right to terminate the Contract at any time without reason or liability.

**11.4 When the Buyer can end the Contract**

11.4.1 If any of the following events happen, the Buyer has the right to immediately terminate its Contract by issuing a termination notice in writing to the Supplier and the consequences of termination in clause 11.5.1 shall apply:

11.4.1.1 there's a Supplier Insolvency Event;

11.4.1.2 the Supplier is in Material Breach of the Contract and does not cure such breach within 30 days of Buyer's written notice;

11.4.1.3 intentionally omitted;

11.4.1.4 the Supplier or its affiliates embarrass or bring the Buyer into disrepute or diminish the public trust in them, to the extent that it constitutes a Material Breach of the Contract; or

11.4.1.5 the Supplier fails to comply with its legal obligations in the fields of environmental, social or employment Law when providing the Deliverables, to the extent that it constitutes a Material Breach of the Contract.

**11.5 What happens if the Contract ends**

11.5.1 Where the Buyer terminates the Contract under clause 1.9 of Annex 5, 11.4, 7.8.2, 32.4 all of the following apply:

11.5.1.1 Intentionally omitted;

11.5.1.2 the Buyer's payment obligations under the terminated Contract stop immediately;

11.5.1.3 accumulated rights of the Parties are not affected;

11.5.1.4 the Supplier must promptly delete or return the Government Data other than Government Data (i) that is Personal Data in respect of which the Supplier is a Controller; (ii) in respect of which the Supplier has rights to hold the Government Data independently of this Contract; and (iii) where required to retain copies by Law;

11.5.1.5 the Supplier must promptly return any of the Buyer's property provided under the Contract;

11.5.1.6 the Supplier must, at no cost to the Buyer, give all reasonable assistance to the Buyer as described in GitLab's Documentation and enable Buyer to export data in structured, commonly-used formats; and

11.5.1.7 the Supplier must refund to the Buyer the pro-rated Charges that it has been paid in advance for Deliverables that it has not provided as at the date of termination or expiry.

11.5.2 The following clauses survive the expiry or termination of the Contract: 1, 5, 7.2, 8.4, 8.5, 11.5, 11.6.3, 12, 14, 15, 16, 18, 19, 22, 31.2.2, 35, 36 and Annex 5 and any clauses which are expressly or by implication intended to continue.

**11.6 When the Supplier can end the Contract and what happens when the contract ends (Buyer and Supplier termination)**

11.6.1 The Supplier can issue a reminder notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate the Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over

10% of the total Contract value or £1,000, whichever is the lower, within 30 days of the date of the reminder notice.

11.6.2 The Supplier may terminate this Contract in case of the Buyer's Material Breach of the Contract and does not cure the breach within thirty (30) days after Supplier's written notice.

11.6.3 Where the Buyer terminates the Contract in accordance with clause 11.3 or the Supplier terminates the Contract under clause 11.6 or:

11.6.3.1 the Buyer must promptly pay all unpaid Charges covering the remainder of the Subscription Term of all Order Forms, to the extent permitted by applicable law. For the avoidance of doubt, in no event will termination relieve Buyer of its obligation to pay any Charges payable to Supplier for the period prior to the effective date of termination;

11.6.3.2 Intentionally omitted; and 11.6.3.3

clauses 11.5.1.3 to 11.5.1.6 apply.

11.6.4 Intentionally omitted.

**11.7 Partially ending and suspending the Contract - Not Applicable**

11.7.1 Where the Buyer has the right to terminate the Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends the Contract it can provide the Deliverables itself or buy them from a third party.

11.7.2 The Buyer can only partially terminate or suspend the Contract if the remaining parts of it can still be used to effectively deliver the intended purpose.

11.7.3 The Parties must agree (in accordance with clause 25) any necessary variation required by clause 11.7, but the Supplier may not either:

11.7.3.1 reject the variation; or

11.7.3.2 increase the Charges, except where the right to partial termination is under clause 11.3.

11.7.4 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under clause 11.7.

12. How much you can be held responsible for

12.1 Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more, in aggregate, than 125% of the Charges paid or payable to the Supplier in the one-year period preceding the first incident out of which the liability arose.

12.2 No Party is liable to the other for:

12.2.1 any indirect losses, punitive, special, incidental or consequential damages; and/or

12.2.2 loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

12.3 In spite of clause 12.1, neither Party limits or excludes any of the following:

12.3.1 its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors;

12.3.2 its liability for bribery or fraud or fraudulent misrepresentation by it or its employees; or

12.3.3 any liability that cannot be excluded or limited by Law.

12.4 In spite of clause 12.1, the Supplier's liability arising under clauses 8.4, 9.3.2, or 31.2.2. or clause 1.7 of Annex 5 shall be no more, in the aggregate, than 300% of the Charges paid or payable to the Supplier in the one-year period preceding the first incident out of which the liability arose.

12.5 In spite of clause 12.1, the Buyer's liability arising under clause 8.5. shall be no more, in the aggregate, than 300% of the Charges paid or payable to the Supplier in the one-year period preceding the first incident out of which the liability arose.

12.6 In spite of clause 12.1, but subject to clauses 12.2 and 12.3, the Supplier's total aggregate liability in each Contract Year under clause 14.5.4 is no more than the Data Protection Liability Cap.

12.7 Each Party must use all reasonable endeavours to mitigate any loss or damage which it suffers under or in connection with the Contract, including any indemnities.

12.8 Intentionally omitted.

13. Obeying the Law

13.1 The Supplier, in connection with provision of the Deliverables:

13.1.1 is expected to meet and take reasonable efforts to have its Subcontractors meet applicable standards substantially similar to those set out in the Supplier Code of Conduct: (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1163536/Supplier_Code_of_Conduct_v3.pdff ) as such Code of Conduct may be updated from time to time, and such other sustainability requirements as set out in the Order Form.;

13.1.2 must comply with the provisions of the Official Secrets Acts 1911 to 1989 and section 182 of the Finance Act 1989;

13.1.3 must support the Buyer in fulfilling its Public Sector Equality duty under section 149 of the Equality Act 2010;

13.1.4 must comply with the model contract terms contained in (a) to (l) of Annex C of the guidance to PPN 009 (Tackling Modern Slavery in Government Supply Chains), as such clauses may be amended or updated from time to time; and

13.1.5 meet the applicable Government Buying Standards applicable to Deliverables which can be found online at: https://www.gov.uk/government/collections/sustainable-procurementthe-government-buying-standards-gbs, as updated from time to time.

13.2 The Supplier shall be responsible to the Buyer, in accordance with the terms and conditions of this Contract, for any costs resulting from any default by the Supplier relating to any applicable Law to do with the Contract.

13.3 The Supplier must appoint a compliance officer who must be responsible for ensuring that the Supplier complies with Law.

14. Data Protection and Security

14.1 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.2 The Supplier must ensure that any Supplier, Subcontractor, or Sub-processor system holding any Government Data, including back-up data, is a secure system that materially complies with the Security Requirements (Schedule 16 – Security Buyer-Led Assurance) or as otherwise provided in writing by the Buyer (where any such requirements have been provided).

14.3 If at any time the Supplier suspects or has reason to believe that the Government Data is corrupted, lost or sufficiently degraded, then the Supplier must immediately notify the Buyer and suggest remedial action.

14.4 If the Government Data is any of (i) corrupted, (ii) lost or (iii) sufficiently degraded, in each case as a result of the Supplier's Default, so as to be unusable the Buyer may either or both:

14.4.1 tell the Supplier (at the Supplier's expense) to restore or get restored Government Data as soon as practical and in accordance with the Supplier's Disaster Recovery Plan for Dedicated. https://docs.gitlab.com/administration/dedicated/disaster_recovery/#recovery-objectives ; and/or

14.4.2 Intentionally omitted.

14.5 The Supplier:

14.5.1 must, subject to the Security Requirements (if any), provide the Buyer with all Government Data in an agreed format (provided it is secure and readable) within 10 Working Days of a written request;

14.5.2 must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;

14.5.3 must, subject to the Security Requirements (if any), securely erase (using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted) all Government Data and any copies it or a Subcontractor holds when asked to do so by the Buyer unless required by Law to retain it, other than in relation to Government Data in respect of which the Supplier is a Controller or which the Supplier has rights to hold the Government Data independently of this Contract; and

14.5.4 shall be liable to the Buyer against any and all losses incurred if the Supplier breaches clause 14 or any Data Protection Legislation.

14.6 The Parties acknowledge that for the purposes of the Data Protection Legislation,

the nature of the activity carried out by each of them in relation to their respective obligations under the Contract dictates the status of each party under the DPA 2018. A Party may act as:

14.6.1 "Controller" in respect of the other Party who is "Processor";

14.6.2 "Processor" in respect of the other Party who is "Controller";

14.6.3 "Joint Controller" with the other Party – Not Applicable;

14.6.4 "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under the Contract and shall specify in Part A Authorised Processing Template of Annex 1 – Processing Personal Data which scenario they think shall apply in each situation.

**14.7 Where one Party is Controller and the other Party its Processor**

14.7.1 Where a Party is a Processor, the only processing that the Processor is authorised to do is listed in Part A Authorised Processing Template of Annex 1 – Processing Personal Data by the Controller and may not be determined by the Processor. The term "processing" and any associated terms are to be read in accordance with Article 4 of the UK GDPR and EU GDPR (as applicable).

14.7.2 The Processor must notify the Controller immediately if it thinks the Controller's instructions breach the Data Protection Legislation.

14.7.3 The Processor must give all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment before starting any processing, which may include, at the discretion of the Controller:

14.7.3.1 a systematic description of the expected processing and its purpose;

14.7.3.2 the necessity and proportionality of the processing operations;

14.7.3.3 the risks to the rights and freedoms of Data Subjects; and

14.7.3.4 the intended measures to address the risks, including safeguards, security measures and mechanisms to protect Personal Data and assurance that those measures comply with any Security Requirements.

14.7.4 The Processor must, in in relation to any Personal Data processed under this Contract:

14.7.4.1 process that Personal Data only in accordance with this clause 14, Part A Authorised Processing Template of Annex 1 – Processing Personal Data and Schedule 16 – Security Buyer-Led Assurance unless the Processor is required to do otherwise by Law. If lawful to notify the Controller, the

Processor must promptly notify the Controller if the Processor is otherwise required to process Personal Data by Law before processing it.

14.7.4.2 put in place appropriate Protective Measures to protect against a Data Loss Event which must be approved by the Controller.

14.7.4.3 ensure that:

(a) the Processor Personnel do not process Personal Data except in accordance with clause 14, Part A Authorised Processing Template of Annex 1 – Processing Personal Data and Schedule 16 – Security Buyer-Led Assurance

(b) it uses the Pre-Employment procedures as set out in Schedule 16 Appendix 1, Section 3 to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the Processor's duties under this clause 14 and Schedule 16;

(ii) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(iii) are informed of the confidential nature of the Personal Data and do not provide any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise allowed by the Contract; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data.

(c) the Processor must not transfer Personal Data outside of the UK and/or the EEA unless authorized by the Controller and the following conditions are fulfilled. For the sake of clarity, and subject to section 14.7.11, transfers to Supplier's Subprocessors at https://about.gitlab.com/privacy/subprocessors/ for the Supplier's Dedicated product at are deemed authorized.

(i) the transfer is in accordance with Article 45 of the UK GDPR (or section 74A of DPA 2018)

and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable), provided that if the destination country of a transfer is the United States:

(A) the Supplier shall ensure that prior to the transfer of any Personal Data to the United States relying on this adequacy (including to any United States-based Subcontractors and/or Subprocessors), the Supplier (and/or the applicable Subcontractor and/or Subprocessor) must be selfcertified and continue to be self-certified on the US Data Privacy Framework if the Supplier (and/or the applicable Subcontractor and/or Subprocessor) does not have in place the transfer mechanism described in 14.7.4.3(d) relating to the EU SCCs and the UK International Data Transfer Agreement;

(B) In the event section 14.7.4.3(c)(A) applies, the Supplier shall notify the Buyer immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Subcontractor's or Subprocessor's position on the US Data Privacy Framework (for example if that entity ceases to be certified or is at risk of being so, or there is a strong likelihood of a competent court finding the US Data Privacy Framework unlawful), and the Supplier must then take all appropriate steps to remedy the certification and/or put in place alternative data transfer mechanisms in compliance with this Paragraph 14.7.4.3(c)(i); and

(C) in the event section 14.7.4.3(c)(A) applies and that the Supplier (and/or the applicable Subcontractor or Subprocessor):

(1) ceases to be certified on the US Data Privacy Framework and the Supplier does not put in place the

alternative data transfer mechanisms required for compliance with this Paragraph 14.7.4.3(c)(i);

(2) the US Data Privacy Framework is no longer available and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 14.7.4.3(c)(i); and/or

(3) fails to notify the Buyer of any changes to its certification status in accordance with Paragraph 14.7.4.3(c)(i)(B) above, the Buyer shall have the right to terminate this Contract with immediate effect; or

(d) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) and/or the transfer is in accordance with Article 46 of the EU GDPR (where applicable) as determined by the Controller which could include relevant parties entering into: (i) where the transfer is subject to UK GDPR:

(A) the International Data Transfer Agreement (the "**IDTA**"), as published by the Information Commissioner's Office from time to time under section 119A(1) of the DPA 2018 as well as any additional measures determined by the Controller;

(B) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time ("**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**") as published by the Information Commissioner's Office from time to time; and/or

(ii) where the transfer is subject to EU GDPR, the EU SCCs, as well as any additional measures determined by the Controller being implemented by the importing party;

(e) the Data Subject has enforceable rights and effective legal remedies when transferred;

(f) the Processor meets its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

(g) the Processor complies with the Controller's reasonable prior instructions about the processing of the Personal Data.

14.7.5 The Processor must at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

14.7.6 The Processor, unless legally prohibited, must notify the Controller without undue delay if it:

14.7.6.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

14.7.6.2 receives a request to rectify, block or erase any Personal Data;

14.7.6.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

14.7.6.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;

14.7.6.5 receives a request from any third Party for disclosure of Personal Data where compliance with the request is required or claims to be required by Law; and

14.7.6.6 becomes aware of a Data Loss Event.

14.7.7 Any requirement to notify under clause 14.7.6 includes the provision of further information to the Controller in stages as details become available.

14.7.8 The Processor must promptly provide the Controller with full assistance in relation to any Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 14.7.6. This includes giving the Controller:

14.7.8.1 full details and copies of the complaint, communication or request;

14.7.8.2 reasonably requested assistance so that it can comply with a Data Subject Access Request within the relevant timescales in the Data Protection Legislation;

14.7.8.3 any Personal Data it holds in relation to a Data Subject on request;

14.7.8.4 reasonable assistance that it requests following any Data Loss Event; and

14.7.8.5 assistance that it requests relating to a consultation with, or request from, the Information Commissioner's Office or any other regulatory authority.

14.7.9 The Processor must maintain full, accurate records and information to show it complies with this clause 14. This requirement does not apply where the Processor employs fewer than 250 staff, unless either the Controller determines that the processing:

14.7.9.1 is not occasional;

14.7.9.2 includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

14.7.9.3 is likely to result in a risk to the rights and freedoms of Data Subjects.

14.7.10 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

14.7.11 Before allowing any Subprocessor to process any Personal Data, the Processor must:

14.7.11.1 notify the Controller in writing of any changes to the Subprocessor List at thirty (30) days (https://about.gitlab.com/privacy/subprocessors/) in advance of the intended Subprocessor and processing. Controller agrees that it will subscribe to receive Subprocessor alerts at https://about.gitlab.com/privacy/subprocessors/#signup, which will satisfy the notice obligation of this paragraph;

14.7.11.2 make a commercially reasonable change to the Controller's configuration or use of the Services if Controller objects to the change in Subprocessor within the thirty (30) day notice period referred to in the preceding paragraph. If Controller does not object within the thirty (30) day period prior to onboarding the new Subprocessor, Processor shall consider the new Subprocessor approved by Controller;

14.7.11.3 enter into a written contract with the Sub-processor so that a substantially equivalent data processing agreement to this clause 14 applies to the Sub-processor; and

14.7.11.4 provide the Controller with any information about the Subprocessor that the Controller reasonably requires.

14.7.12 The Processor remains fully liable for all acts or omissions of any Subprocessor.

14.7.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office or any other regulatory authority.

**14.8 Joint Controllers of Personal Data – Not Applicable**

In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Part B Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data.

**14.9 Independent Controllers of Personal Data**

In the event that the Parties are Independent Controllers in respect of Personal Data under the Contract, the terms set out in Part C Independent Controllers (Optional) of Annex 1 – Processing Personal Data shall apply to this Contract. 15. What you must keep confidential

15.1 Each Party must:

15.1.1 keep all Confidential Information it receives confidential and secure;

15.1.2 not disclose, use or exploit the disclosing Party's Confidential Information without the disclosing Party's prior written consent, except for the purposes anticipated under the Contract; and

15.1.3 immediately notify the disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

15.2 In spite of clause 15.1, a Party may disclose Confidential Information which it receives from the disclosing Party in any of the following instances:

15.2.1 where disclosure is required by applicable Law if the recipient Party notifies the disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;

15.2.2 if the recipient Party already had the information without obligation of confidentiality before it was disclosed by the disclosing Party;

15.2.3 if the information was given to it by a third party without obligation of confidentiality;

15.2.4 if the information was in the public domain at the time of the disclosure through no fault of the Receiving Party;

15.2.5 if the information was independently developed without reliance upon the disclosing Party's Confidential Information;

15.2.6 on a confidential, need-to-know basis, to its auditors or for the purposes of regulatory requirements;

15.2.7 on a confidential, need-to-know basis, to its professional advisers on a need-to-know basis; and

15.2.8 to the Serious Fraud Office where the recipient Party has reasonable grounds to believe that the disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. Either Party shall remain responsible at all times for compliance with the confidentiality obligations set out in this Contract by the persons to whom they have made the disclosure.

15.4 The Buyer may disclose Confidential Information in any of the following cases:

15.4.1 on a confidential, need-to-know basis to the employees, agents, consultants and contractors of the Buyer;

15.4.2 on a confidential, need-to-know basis to any Crown Body, any successor body to a Crown Body or any company that the Buyer transfers or proposes to transfer all or any part of its business to;

15.4.3 if the Buyer (acting reasonably) considers disclosure legally necessary to carry out its statutory public functions provided that: (a) the Buyer gives the Supplier no less than 14 days' prior written notice; (b) the Buyer consults with the Supplier and considers its objections; (c) disclosure is limited to the minimum extent necessary; (d) disclosure is only to authorized persons with equivalent confidentiality obligations; and (e) the Supplier may propose redactions of commercially sensitive information (f) such disclosure shall in no event result in publication or public release of the Supplier's confidential information;

15.4.4 where requested by Parliament, provided that the same caveats set out in clause 15.4.3 shall apply; and

15.4.5 under clauses 5.8 and 16.

15.5 For the purposes of clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in clause 15.

15.6 Transparency Information and any information which is disclosed under clause 16 is not Confidential Information. To the extent that it is allowed to do so under applicable laws, the Buyer will notify the Supplier prior to publishing any Transparency Information which may contain sensitive commercial information (as defined in section 94 of the Procurement Act 2023) and/or provide the Supplier with a reasonable opportunity to propose redactions to any Transparency Information to protect any sensitive commercial information. However, the extent, content and format of any publication shall be decided by the Buyer, in its sole discretion, provided that such publication shall be limited to the minimum extent required by applicable law, shall preserve confidentiality to the maximum extent legally permissible, and shall not waive any applicable legal privileges or protections.

15.7 The Supplier must not make any press announcement or publicise the Contract or any part of it in any way, without the prior written consent of the Buyer and must take all reasonable endeavours to ensure that Supplier Staff do not either.

16. When you can share information

16.1 The Supplier must tell the Buyer within 5 Working Days if it receives a Request For Information, to the extent legally allowed to do so.

16.2 In accordance with a reasonable timetable and in any event within 5 Working Days of a request from the Buyer, at no additional cost, the Supplier must give the Buyer reasonable co-operation and information needed so the Buyer can:

16.2.1 comply with any Request For Information; and

16.2.2 comply with any of its obligations in relation to publishing Transparency Information.

16.3 Any such reasonable co-operation and/or information from the Supplier shall be provided at no additional cost.

16.4 To the extent that it is allowed to do so under applicable laws, the Buyer will (i) notify the Supplier of a Request For Information at least 10 days prior to making any determination with respect to the Request for Information, (ii) work with the Supplier to decide whether to publish information under clause 16, including by considering in good faith any representation made by the Supplier, and (iii) provide a clear justification for any decision relating to the Request for Information. However, the extent, content and format of the

disclosure shall be decided by the Buyer, in its sole discretion, provided that such disclosure shall be limited to the minimum extent required by applicable law, shall preserve confidentiality to the maximum extent legally permissible, and shall not waive any applicable legal privileges or protections.

17. Insurance

17.1 The Supplier shall ensure it has adequate insurance cover for this Contract.

18. Invalid parts of the contract

18.1 If any provision or part-provision of this Contract is or becomes invalid, illegal or unenforceable for any reason, such provision or part-provision shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Contract. The provisions incorporated into the Contract are the entire agreement between the Parties. The Contract replaces all previous statements, or agreements whether written or oral. No other provisions apply.

19. Other people's rights in the contract

19.1 No third parties may use the Contracts (Rights of Third Parties) Act ("**CRTPA**") to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

19.2 Intentionally Omitted.

20. Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its nonmonetary obligations under the Contract while the inability to perform continues and such Party shall:

20.1.1 provides written notice to the other Party; and

20.1.2 uses all reasonable measures practical to reduce the impact of the Force Majeure Event.

20.2 Any failure or delay by the Supplier to perform its obligations under the Contract that is due to a failure or delay by an agent, Subcontractor and/or Supplier Staff will only be considered a Force Majeure Event if that third party is itself prevented from complying with an obligation to the Supplier due to a Force Majeure Event.

20.3 Either Party can terminate the Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously and the consequences of termination in clauses 11.5.1.2 to 11.5.1.7 shall apply.

20.4 Where a Party terminates under clause 20.3:

20.4.1 each Party must cover its own losses except for termination for Force Majeure as defined under point c) of the Force Majeure definition, in which case Buyer shall not be entitled to credit or refund and remains responsible for all amounts due and payable under the Contract as of the date of termination; and

20.4.2 clauses 11.5.1.2 to 11.5.1.7 apply, except for 20.4.1 where clauses 11.5.1.3 to 11.5.1.6 apply.

21. Relationships created by the contract

21.1 The Contract does not create a partnership, joint venture or employment relationship. The Parties must represent themselves accordingly and ensure others do so.

22. Giving up contract rights

22.1 A partial or full waiver or relaxation of the terms of the Contract is only valid if it is stated to be a waiver in writing to the other Party.

23. Transferring responsibilities

23.1 Neither Party can assign, novate or in any other way dispose of the Contract or any part of it without the other Party's prior written consent, such consent not to be unreasonably withheld or delayed.

23.2 Intentionally omitted.

23.3 Intentionally omitted.

23.4 Intentionally omitted.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

24. Supply Chain

24.1 The Supplier shall be entitled to use the Subcontractors listed at https://about.gitlab.com/privacy/subprocessors/ for the Service. If Supplier wishes to add a new Subcontractor to the list, Supplier will update the list on the website. Buyer may subscribe at https://about.gitlab.com/privacy/subprocessors/#sign-up to receive email notifications of updates to the list, which will serve as written notice to Buyer. If Buyer wishes to object to the approval of a new Subcontractor, meaning an organization or entity not previously listed at https://about.gitlab.com/privacy/subprocessors/, it must provide such objection in writing to GitLab within thirty (30) days after notice has been

received. The Buyer may object to the appointment of a Subcontractor if substantiated evidence suggests that:

24.1.1 the appointment of a proposed Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

24.1.2 the proposed Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

24.1.3 the proposed Subcontractor employs unfit persons.

24.2 If Buyer objects to the change in Subcontractors, the Parties will work together in

good faith to resolve the objection, including making a commercially reasonable change to Customer's configuration or use of the Services to avoid the provision of Services by the new Sub-processor. If the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of all such Subcontractors at all levels of the supply chain including:

24.2.1 their name;

24.2.2 the scope of their appointment; and

24.2.3 the duration of their appointment.

24.3 The Supplier must exercise due skill and care when it selects and appoints Subcontractors.

24.4 Intentionally omitted.

24.5 Intentionally omitted.

24.6 The Supplier shall be fully responsible and liable for all acts and omissions of its subcontractors, as if they were the acts and omissions of the Supplier itself. The engagement of subcontractors shall not relieve the Supplier of any of its obligations or liabilities under this Contract, and the Supplier shall ensure that appropriate contractual arrangements are in place with all subcontractors to enable the Supplier to comply with its obligations under this Contract.

24.7 The Supplier is responsible for all acts and omissions of its Subcontractors and those employed or engaged by them as if they were its own.

25. Changing the contract

25.1 Either Party can request a variation to the Contract which is only effective if agreed in writing and signed by both Parties. Neither Party is required to accept a variation request made by the other Party.

26. How to communicate about the contract

26.1 All notices under the Contract shall be in writing and be served by e-mail unless it is not practicable to do so. An e-mail is effective at 9am on the first Working Day after sending unless an error message is received.

26.2 If it is not practicable for a notice to be served by e-mail in accordance with clause

26.1, notices can be served to the Buyer my means of personal delivery or Prepaid, Royal Mail Signed For™ 1st Class or other prepaid, next Working Day service providing proof of delivery. If either of these options are used to serve a notice, such notices are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise, the notice is effective on the next Working Day.

26.3 Notices to the Buyer or Supplier must be sent to their e-mail address (or address, where e-mail is not practicable) in the Order Form.

26.4 This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

27. Dealing with claims

27.1 If a Beneficiary becomes aware of any Claim, then it must promptly notify the Indemnifier in writing.

27.2 The Beneficiary must:

27.2.1 allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim;

27.2.2 give the Indemnifier reasonable assistance with the Claim if requested; and

27.2.3 not make admissions about the Claim without the prior written consent of the Indemnifier which cannot be unreasonably withheld or delayed.

27.3 The Indemnifier must:

27.3.1 consider and defend the Claim diligently and in a way that does not damage the Beneficiary's reputation; and

27.3.2 not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay, unless the settlement includes a legally binding and unconditional release of the Buyer from all liability and does not adversely affect the Buyer’s reputation or statutory obligations.

28. Equality, diversity and human rights

28.1 The Supplier must follow all applicable employment and equality Law when they perform their obligations under the Contract, including:

28.1.1 protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and

28.1.2 any other requirements and instructions which the Buyer reasonably imposes related to equality Law.

28.2 The Supplier must use all reasonable endeavours, and inform the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on the Contract.

29. Health and safety

29.1 The Supplier must perform its obligations meeting the requirements of:

29.1.1 all applicable Law regarding health and safety; and

29.1.2 the Buyer's current health and safety policy while at the Buyer's premises, as provided to the Supplier.

29.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer premises that relate to the performance of the Contract.

30. Environment and sustainability

30.1 In performing its obligations under the Contract, the Supplier shall, to the reasonable satisfaction of the Buyer:

30.1.1 meet, in all material respects, the requirements of all applicable Laws regarding the environment; and

30.1.2 shall maintain environmental practices substantially similar to those set out in the Buyer's current environmental policy, which the Buyer must provide, to the extent such practices are applicable to the Supplier's in accordance with applicable environmental laws and regulations. The Supplier shall make Supplier Staff aware of applicable environmental requirements relating to their duties under this Contract.

31. Tax

31.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. The Buyer cannot terminate the Contract where the Supplier has not paid a minor tax or social security contribution.

31.2 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under the Contract, the Supplier must both:

31.2.1 comply with the Income Tax (Earnings and Pensions) Act 2003, the Social Security Contributions and Benefits Act 1992 and all other statutes and regulations relating to income tax and National Insurance contributions (including IR35); and

31.2.2 remain liable towards the Buyer for any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Term in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

31.3 At any time during the Term, the Buyer may reasonably specify information that the Supplier must provide with regard to the Supplier, the Supplier Staff, the Workers, or the Supply Chain Intermediaries and set a reasonable deadline for responding, which:

31.3.1 If and to the extent applicable, demonstrates that the Supplier, Supplier Staff, Workers, or Supply Chain Intermediaries comply with the legislation specified in Clause 31.2.1, or why those requirements do not apply; and

31.3.2 assists with the Buyer's due diligence, compliance, reporting, or demonstrating its compliance with any of the legislation in Clause 31.2.1.

31.4 The Buyer may supply any information they receive from the Supplier under Clause
31.3 to HMRC for revenue collection and management and for audit purposes.

31.5 The Supplier must, upon request, inform the Buyer of any Workers or Supplier Staff providing services to the Buyer who are contracting, begin contracting, or stop contracting via an intermediary which meets one of conditions A-C set out in section 61N of the Income Tax (Earnings and Pensions) Act 2003 and/or Regulation 14 of the Social Security Contributions (Intermediaries) Regulations 2000.

31.6 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables (provided that "payment relating to the Deliverables" shall not include ordinary salary, wages, or benefits paid under standard employment contracts where such payments are not conditional upon, additional to, or specifically attributable to the performance of Services for the Buyer), then the Supplier must take reasonable steps to ensure that any contract with the Worker that the Supplier enters into after the Start Date contains requirements that:

31.6.1 the Buyer may, at any time during the term of the Contract, request that the Worker provides information which demonstrates they comply with clause 31.2, or why those requirements do not apply, the Buyer can

specify the reasonable information the Worker must provide and the reasonable deadline for responding;

31.6.2 the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;

31.6.3 the Worker's contract may be terminated at the Buyer's request if the Worker provides information which confirms that the Worker is not complying with the requirements in clause 31.2; and

31.6.4 the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

32. Conflict of interest

32.1 The Supplier must take reasonable action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of a Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to the Buyer if it becomes aware a Conflict of Interest happens or is expected to happen.

32.3 The Buyer and Supplier will discuss in good faith whether there are any reasonable steps that can be put in place to mitigate or resolve such Conflict of Interest. If, in the reasonable opinion of the Buyer, such steps cannot resolve a Conflict of Interest within 30 days, the Buyer may terminate the Contract immediately by giving notice in writing to the Supplier where there is a Conflict of Interest and, subject to clause 32.4, where the reason for the unresolvable Conflict of Interest is in the reasonable opinion of the Buyer

32.3.1 outside of the control of the Supplier, clauses 11.5.1.2 to 11.5.1.7 shall apply

32.3.2 within the control of the Supplier, the whole of clause 11.5.1 shall apply.

32.4 Where the Supplier knew or reasonably should have known about a Conflict of Interest and has deliberately or negligently failed to notify the Buyer about a Conflict of Interest and the Buyer terminates under clause 32.3, the whole of clause 11.5.1 shall apply.

33. Reporting a breach of the contract

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to the Buyer

any material breach of Law, clause 13.1, or clauses 27 to 32 that could reasonably be expected to have a significant adverse impact on the Services or the Buyer's interests.

33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in clause 33.1 to the Buyer or a Prescribed Person.

34. Further Assurances

34.1 Each Party will, at the request and cost of the other Party, do all things which may be reasonably necessary to give effect to the meaning of this Contract.

35. Resolving disputes

35.1 If there is a dispute between the Parties, their senior representatives with full and final authority to settle the dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the dispute by commercial negotiation.

35.2 If the dispute is not resolved within 30 days of the initial meeting under clause 35.1, the Parties may refer the matter to mediation using the Centre for Effective Dispute Resolution ("**CEDR**") Model Mediation Procedure current at the time of the dispute. If the Parties cannot agree on a mediator within 14 days of referring the matter to mediation, the mediator will be nominated by CEDR. If either Party does not wish to proceed with mediation, or mediation does not resolve the dispute, the dispute must be resolved using clauses 35.3 to 35.5.

35.3 Unless either Party refers the dispute to arbitration using clause 35.4, the Parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction.

35.4 Each Party may refer any dispute to be finally resolved by arbitration under the London Court of International Arbitration ("LCIA") Rules current at the time of the dispute. The arbitration will be conducted by a sole arbitrator unless (a) the amount in dispute exceeds £1,000,000, in which case either Party may request a threearbitrator tribunal; or (b) the LCIA Court determines that in the circumstances a three-member tribunal is appropriate. The seat or legal place of the arbitration will be London and the proceedings will be in English.

35.5 Intentionally omitted.

35.6 The Supplier cannot suspend the performance of the Contract during any dispute, unless it would be unreasonable to expect the Supplier to continue performance having regard to all the circumstances, including but not limited to third party intellectual property claims, regulatory requirements, safety concerns, or material breach or non-payment by the Buyer.

36. Which law applies

36.1 This Contract and any issues or disputes arising out of, or connected to it, are governed by English law.

# V. Annex 1 – Processing Personal Data

## 1 Authorised Processing Template

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

The contact details of the Controller's Data Protection Officer are: [redacted]

The contact details of the Processor's Data Protection Officer are: [redacted]

The Processor shall comply with any further written instructions with respect to processing by the Controller.

Any such further instructions shall be incorporated into this Annex.

| Description | Details |
|---|---|

| | |
|---|---|
| Identity of Controller for each Category of Personal Data | **The Buyer is Controller and the Supplier is Processor**<br>The Parties acknowledge that in accordance with Paragraph **Error! Reference source not found.** and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:<br>• Account Information, such as name, username, email address, and password<br>● Profile Information, such as name, public avatar or photo, employer, email address, job title, address, social media handles, and biography<br>● Contact information, such as name, address, email address, and telephone<br>● Content provided through the use of the Services, such as repositories, issues, commits, project contributions, comments, and input/output related to AI-powered features<br>● Customer Support Information, such as the request you are making or the services being provided |

| **Description** | **Details** |
|---|---|

| | |
|---|---|
| | ● Product Analytics for Customer to measure engagement by their own use<br>**The Parties are Independent Controllers of Personal Data**<br>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:<br>● Personally identifiable information *of* Supplier Staff for which the Supplier is the Controller,<br>● Personally identifiable information of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Staff) engaged in the performance of the Buyer's duties under this Contract) for which the Buyer is the Controller,<br>● Personal Data in a pseudonymized format related to Buyer's Users' usage of the product, such as user click rates, feature usage and other metrics listed here https://metrics.gitlab.com/events.<br>● Personal Data of Buyer's users for the purposes of preventing fraud, abuse or other security violations as required under law. |
| Subject matter of the Processing | **Where Buyer is Controller and the Supplier is Processor**, the subject matter relates to Buyer's use of the software Services for the purposes determined by Buyer in its sole discretion.<br>**Where the Parties are Independent Controllers of Personal Data**, the Processing allows for Supplier to understand how the Services are used, to process payments for the Services, to administer the Services, to comply with legal obligations, and to protect the safety and property of Supplier and Buyer. |

| **Description** | **Details** |
|---|---|

| | |
|---|---|
| Duration of the Processing | **Where Buyer is Controller and the Supplier is Processor,** Personal data will be retained for the period determined by Buyer, including until termination of the Subscription Term, subject to exceptions allowed by law and under the applicable Agreements with Buyer.<br><br>**Where the Parties are Independent Controllers of Personal Data** Personal Data will be retained for the described in the Data Retention section of Supplier's Privacy Statement and in accordance with our Records Retention Policy posted at https://handbook.gitlab.com/handbook/legal/record-retention-policy/. For pseudonymized product usage data, Supplier retains this data for 3-years from the point of collection. |
| Nature and purposes of the Processing | **Where Buyer is Controller and the Supplier is Processor,** the Processing relates to Buyer's use of the Services for purposes determined and controlled by Buyer in its sole discretion.<br><br>**Where the Parties are Independent Controllers of Personal Data, the** Processing allows for Supplier to understand how the Services are used, to process payments for the Services, to administer the Services, to comply with legal obligations, and to protect the safety and property of Supplier and Buyer. |
| Type of Personal Data being Processed | **Where Buyer is Controller and the Supplier is Processor**<br>• Account Information, such as name, username, email address, and password |

| Description | Details |
| --- | --- |
| | ● Profile Information, such as name, public avatar or photo, employer, email address, job title, address, social media handles, and biography<br>● Contact information, such as name, address, email address, and telephone<br>● Content provided through the use of the Services, such as repositories, issues, commits, project contributions, comments, and input/output related to AI-powered features<br>● Customer Support Information, such as the request you are making or the services being provided<br>● Product Analytics for Customer to measure engagement by their own use<br><br>**Where the Parties are Independent Controllers of Personal Data**<br>• Account Management Information, such as license data, historical user data, and account administrator contact information<br>• Billing Information, such as Customer's billing address, billing contact, and credit card or banking information<br>• Customer Product Usage Information, such as feature usage and engagement metrics found at https://metrics.gitlab.com/events<br>• Security and Fraud Prevention Information, such as log data, device data and IP address |

| | |
|---|---|
| Categories of Data Subject | **Where Buyer is Controller and the Supplier is Processor**<br>• Buyer's prospects, clients, business partners, and vendors (who are natural persons)<br>• Buyer's employees, agents, advisors and freelancers (who are natural persons)<br>• Buyer's users authorized by Buyer to use the Services<br>• Any other natural persons who become identifiable through content provided via Buyer's use of the Services<br><br>**Where the Parties are Independent Controllers of Personal Data**<br>• Buyer's employees, agents, advisors and freelancers (who are natural persons) |

| **Description** | **Details** |
|---|---|
| | • Buyer's users authorized by Buyer to use the Services |
| Plan for return and destruction of the data once the Processing is complete<br>UNLESS requirement under law to preserve that type of data | **Where Buyer is Controller and the Supplier is Processor**<br><br>Personal data will be retained for the period determined by Buyer, including until termination of the Subscription Term, subject to exceptions allowed by law and under the applicable Agreements with Buye<br>**Where the Parties are Independent Controllers of Personal Data**<br>Personal Data will be retained for the described in the Data Retention section of Supplier's Privacy Statement and in accordance with our Records Retention Policy posted at https://handbook.gitlab.com/handbook/legal/record-retention-policy/. For pseudonymised product usage data, Supplier retains this data for 3-years from the point of collection. |

| | |
|---|---|
| Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Contract and international transfers and legal gateway | **Where Buyer is Controller and the Supplier is Processor**<br><br>Location for Buyer's content will be the Dedicated location of Buyer's choosing. For Customer Support information, Customer Support data will be hosted in the United States but may be accessed Supplier's globally distributed workforce to render Customer Support. The transfer mechanism relied on for data processing to the United States is the IDTA within Annex 6 of this contract<br><br>**Where the Parties are Independent Controllers of Personal Data** |
| **Description** | **Details** |
| | Buyer's data will be hosted and access from the United States The transfer mechanism relied on for data processing to the United States is the IDTA within Annex 6 of this contract |

| | |
|---|---|
| Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect Personal Data processed under this Contract Agreement against a breach of security (insofar as that breach of security relates to data) or a Data Loss Event (noting that any Protective Measures are to be in accordance with any Security Requirements) | Supplier will implement and maintain the following security measures:<br><br>• Those Technical and Organisational Security Measures for GitLab cloud services found at https://handbook.gitlab.com/handbook/security/securityassurance/technical-and-organizational-measures/.<br>• Those policies and certifications found in our Trust Center (https://trust.gitlab.com/).<br>• Sub-processors will implement and maintain security measures substantively similar to those listed on the Supplier's Technical and Organisational measures page and the Trust Center. |

## 2 Joint Controller Agreement *(Not Used)*

## 3 Independent Controllers

## 1. INDEPENDENT CONTROLLER PROVISIONS

1.1 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their processing of such Personal Data as Controller.

1.2 Each Party shall process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

1.3 Where a Party has provided Personal Data to the other Party in accordance with Paragraph **Error! Reference source not found.** of this **Error! Reference source not found. Error! Reference source not found.** of **Error! Reference source not found.** above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

1.4 The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the processing of Personal Data for the purposes of the Contract.

1.5 The Parties shall only provide Personal Data to each other:

1.5.1 to the extent necessary to perform their respective obligations under the Contract;

1.5.2 in compliance with the Data Protection Legislation (including by ensuring all required fair processing information has been given to affected Data Subjects);

1.5.3 where the provision of Personal Data from one Party to another involves transfer of such data to outside the UK and/or the EEA, if the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

1.5.3.1 the destination country (and if applicable the entity receiving the Personal Data) has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74A and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable), provided that if the destination country of a transfer is the United States:

(a) the Supplier shall ensure that prior to the transfer of any Personal Data to the United States relying on this adequacy (including to any United States-based Subcontractors and/or Subprocessors), the Supplier

(and/or the applicable Subcontractor and/or Subprocessor) must be self-certified and continue to be self-certified on the US Data Privacy Framework if the Supplier (and/or the applicable Subcontractor and/or Subprocessor) does not have in place the transfer mechanism described in 1.5.3.2 relating to the EU SCCs and the UK International Data Transfer Agreement;

(b) in the event section 1.5.3.1(a) applies, the Supplier shall notify the Buyer immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Subcontractor's or Subprocessor's position on the US Data Privacy Framework (for example if that entity ceases to be certified or is at risk of being so, or there is a strong likelihood of a competent court finding the US Data Privacy Framework unlawful), and the Supplier must then take all appropriate steps to remedy the certification and/or put in place alternative data transfer mechanisms in compliance with this Paragraph 0; and

(c) in the event section 1.5.3.1(a) applies and that the Supplier (and/or the applicable Subcontractor or Subprocessor):

(i) ceases to be certified on the US Data Privacy Framework and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 0;

(ii) the US Data Privacy Framework is no longer available and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 0; and/or

(iii) fails to notify the Buyer of any changes to its certification status in accordance with Paragraph 1.5.3.1(b) above, the Buyer shall have the right to terminate this Contract with immediate effect; or

1.5.3.2 the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75

and/or Article 46 of the EU GDPR (where applicable)) as determined by the non-transferring Party which could include the parties entering into:

(a) where the transfer is subject to UK GDPR:

(i) the UK International Data Transfer Agreement (the "**IDTA**"), as published by the Information Commissioner's Office or such updated version of such IDTA as is published by the Information Commissioner's Office under section 119A(1) of the DPA 2018 from time to time; or

(ii) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time (the "**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**") as published by the Information Commissioner's Office from time to time; and/or

(b) where the transfer is subject to EU GDPR, the EU SCCs; as well as any additional measures determined by the nontransferring Party being implemented by the importing party;

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

1.5.3.4. the transferring Party 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 non-transferring Party in meeting its obligations); and

1.5.3.5 the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring

Party with respect to the processing of the Personal Data; and

1.5.4 where it has recorded it in **Error! Reference source not found. Error! Reference source not found.** of **Error! Reference source not found.**.

1.6 Taking into account the state of the art, the costs of implementation and the nature,

scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

1.7 A Party processing Personal Data for the purposes of the Contract shall maintain a

record of its processing activities in accordance with Article 30 UK GDPR and shall make the applicable portions of such record available to the other Party upon reasonable request.

1.8 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract ("**Request Recipient**"):

1.8.1 the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

1.8.2 where the request or correspondence is directed to the other Party and/or relates to that other Party's processing of the Personal Data, the Request Recipient will:

1.8.2.1 promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

1.8.2.2 provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

1.9 Each Party shall promptly notify the other Party upon it becoming aware of any Data Loss Event relating to Personal Data provided by the other Party pursuant to the Contract and shall:

1.9.1 do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Data Loss Event;

1.9.2 implement any measures necessary to restore the security of any compromised Personal Data;

1.9.3 work with the other Party to make any required notifications to the Information Commissioner's office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

1.9.4 not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

1.10 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in **Error! Reference source not found. Error! Reference source not found.** of **Error! Reference source not found.**.

1.11 Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in **Error! Reference source not found. Error! Reference source not found.** of **Error! Reference source not found.**.

1.12 Notwithstanding the general application of clauses **Error! Reference source not found.** to **Error! Reference source not found.** of the Conditions to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs **Error! Reference source not found.** to 1.12 of this **Error! Reference source not found. Error! Reference source not found.** of **Error! Reference source not found.**.

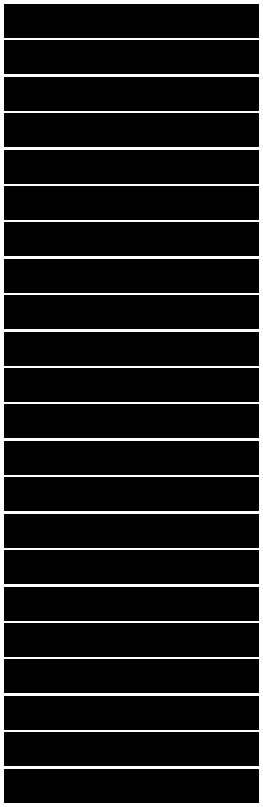
## VI. Annex 2 – Specification

[redacted]

[redacted]

For the avoidance of doubt, this Annex 2 Specifications is provided as a summary for the purchase of GitLab Products by the Buyer through AWS Marketplace.

## VII. Annex 3 – Charges



For the avoidance of doubt, this Annex 3 Charges is provided as a summary for the purchase of GitLab Products by the Buyer through AWS Marketplace. The Payment Method and Payment Term shall be subject to the AWS Marketplace terms agreed to between AWS and the Buyer.

## VIII. Annex 4 – Supplier Tender (Not Used)

# IX. Annex 5 – Optional IPR Clauses *(Optional)*

## Part B- Supplier ownership of New IPR with Buyer rights for the current Contract and broader public sector functions

1. Intellectual Property Rights ("IPRs")

1.1 Each Party keeps ownership of its own Existing IPRs. Any New IPR created under the Contract is owned by the Supplier. The Supplier gives the Buyer a nonexclusive, non- transferable, non-sublicensable licence to use the Supplier's Software licensed under this Contract to enable the Buyer to receive and use the

Deliverables for its own internal business purpose relating to the exercise of the Buyer's (or, if the Buyer is a Public Sector Body, any other Public Sector Body's) business or function, in accordance with the terms of this Contract and in particular, Special Terms 1. For the purposes of this clause "**Public Sector Body**" means a formally established organisation that is (at least in part) publicly funded to deliver a public or government service.

1.2 Intentionally omitted.

1.3 The Buyer gives the Supplier a royalty-free, non-exclusive, non-transferable licence to use, copy, and adapt any Existing IPRs for the purpose of fulfilling its obligations during the Term. This licence is sub-licensable to a Subcontractor for the purpose of enabling the Supplier to fulfil its obligations under the Contract, and in that case the Subcontractor must enter into a confidentiality undertaking with the Supplier on terms no less stringent as set out in clause 15 (What you must keep confidential).

1.4 No New IPR is in scope for this Contract.

1.5 Intentionally omitted.

1.6 Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in this Part or otherwise agreed in writing.

1.7 If any claim is made against the Buyer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Deliverables (an "**IPR Claim**"), then the Supplier indemnifies the Buyer in accordance with Clause 10 of Special Term 1.

1.8 If an IPR Claim is made or anticipated, the Supplier must at its own option and expense, either:

1.8.1 obtain for the Buyer the rights in clause Part B without infringing any third party intellectual property rights; and

1.8.2 replace or modify the relevant item with substitutes that don't infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.

1.9 If in the reasonable opinion of the Supplier neither of the foregoing options is commercially reasonable in order to resolve the IPR Claim within a reasonable time, the Supplier may give written notice that it terminates the Contract from the date set out in the notice, or where no date is given in the notice, the date of the notice. On termination, the consequences of termination in clause 11.5.1 shall apply.

1.10 Intentionally omitted.

1.11 In spite of any other provisions of the Contract and for the avoidance of doubt, award of this Contract by the Buyer and the ordering of any Deliverable under it, does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977, Section 12 of the Registered Designs Act 1949 or Sections 240 – 243 of the Copyright, Designs and Patents Act 1988.

## X. Annex 6 – International Data Transfer Agreement (IDTA)

1. The parties agree that the International Data Transfer Agreement (IDTA), annexed hereto as Annex 6, shall apply to all restricted transfers of personal data under this agreement.

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

# International Data Transfer Agreement

**VERSION A1.0, in force 21 March 2022**

This IDTA has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

## Part 1: Tables

**Table 1: Parties and signatures**

| | | |
|---|---|---|
| **Start date** | 25/09/2025 | |
| **The Parties** | **Exporter (who sends the Restricted Transfer)** | **Importer (who receives the Restricted Transfer)** |

| | | |
|---|---|---|
| **Parties' details** | Full legal name: His Majesty's Revenue and Customs<br>Trading name (if different): HMRC<br>Main address (if a company registered address): 100 Parliament Street<br>London<br>England SW1A 2BQ<br>United Kingdom | Full legal name: GitLab UK limited<br>Trading name (if different):<br>Main address (if a company registered address): Suite 4, 7TH Floor 50 Broadway London, SW1H 0DB, United Kingdom |

| | | |
|---|---|---|
| | Official registration number (if any) (company number or similar identifier): | Official registration number (if any) (company number or similar identifier): |
| **Key Contact** | Full Name (optional): [redacted]<br>Job Title: [redacted]<br>Contact details including email: [redacted] | Full Name (optional): [redacted]<br>Job Title: [redacted]<br>Contact details including email: [redacted] |
| **Importer Data Subject Contact** | | Job Title: GitLab DPO office<br>Contact details including email: [redacted] |
| **Signatures confirming each Party agrees to be bound by this IDTA** | Signed for and on behalf of the **Exporter** set out above<br>Signed: [redacted]<br>Date of signature: [redacted]<br>Full name: [redacted]<br>Job title: [redacted] | Signed for and on behalf of the **Importer** set out above<br>Signed: [redacted]<br>Date of signature: [redacted]<br>Full name: [redacted]<br>Job title: [redacted] |

**Table 2: Transfer Details**

| | |
|---|---|
| **UK country's law that governs the IDTA:** | X England and Wales<br>☐ Northern Ireland<br>☐ Scotland |
| **Primary place for legal claims to be made by the Parties** | X England and Wales<br>☐ Northern Ireland<br>☐ Scotland |

| | |
|---|---|
| **The status of the Exporter** | In relation to the Processing of the Transferred Data:<br>X Exporter is a Controller<br>☐ Exporter is a Processor or Sub-Processor |
| **The status of the Importer** | In relation to the Processing of the Transferred Data:<br>X Importer is a Controller<br>X Importer is the Exporter's Processor or Sub-Processor<br>☐ Importer is **not** the Exporter's Processor or SubProcessor (and the Importer has been instructed by a Third Party Controller) |
| **Whether UK GDPR applies to the Importer** | ☒ UK GDPR applies to the Importer's Processing of the Transferred Data<br>☐ UK GDPR does not apply to the Importer's Processing of the Transferred Data |

| | |
|---|---|
| **Linked Agreement** | **If the Importer is the Exporter's Processor or SubProcessor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data:<br>Name of agreement: Short Form Contract for the Supply of Goods and/or Services<br>Date of agreement: 25th of September, 2025<br>Parties to the agreement: HM Revenue and Customs & Gitlab UK Ltd<br>Reference (if any):<br>**Other agreements** – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:<br>Name of agreement:<br>Date of agreement:<br>Parties to the agreer<br>Reference (if any):<br>**If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which |
| | sets out the Exporter's instructions for Processing the Transferred Data:<br>Name of agreement:<br>Date of agreement:<br>Parties to the agreement:<br>Reference (if any): |

| | |
|---|---|
| **Term** | The Importer may Process the Transferred Data for the following time period:<br>☐ the period for which the Linked Agreement is in force X<br>time period: The length of the contract (39 months)<br>☐ (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose. |
| **Ending the IDTA before the end of the Term** | ☐ the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.<br>☒ the Parties can end the IDTA before the end of the Term by serving:<br>1 months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach). |
| **Ending the IDTA when the Approved IDTA changes** | Which Parties may end the IDTA as set out in Section 29.2:<br>☐ Importer<br>☒ Exporter<br>neither Party<br>☐ |
| **Can the Importer make further transfers of the Transferred Data?** | ☒ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).<br>☐ The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). |

| | |
|---|---|
| **Specific restrictions when the Importer may transfer on the Transferred Data** | The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1:<br>☐ if the Exporter tells it in writing that it may do so.<br>☐ to:<br>☒ to the authorised receivers (or the categories of authorised receivers) set out in: https://about.gitlab.com/privacy/subprocessors/ ☐ there are no specific restrictions. |
| **Review Dates** | ☐ No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date:<br>The Parties must review the Security Requirements at least once:<br>☐ each month(s)<br>☐ each quarter<br>☐ each 6 months<br>☐ each year<br>☐ each year(s)<br>☒ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment |

**Table 3: Transferred Data**

| | |
|---|---|
| **Transferred Data** | The personal data to be sent to the Importer under this IDTA consists of:<br>☐ The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.<br>☒ The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. |

| | |
|---|---|
| **Special Categories of** | The Transferred Data includes data relating to: |
| **Personal Data and criminal convictions and offences** | ☐ racial or ethnic origin ☐ political opinions ☐ religious or ☐ philosophical beliefs ☐ trade union membership ☐ genetic data ☐ biometric data for the purpose of ☐ uniquely identifying a ☐ natural person ☐ physical or mental health ☐ sex life or sexual orientation ☐ criminal convictions and ☐ offences ☐ none of the above ☐ set out in: ☒ ☐ And:<br>☐ The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to.<br>☒ The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. |

| | |
|---|---|
| **Relevant Data Subjects** | The Data Subjects of the Transferred Data are:<br>☐ The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.<br>☒ The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. |
| **Purpose** | ☐ The Importer may Process the Transferred Data for the following purposes:<br>☒ The Importer may Process the Transferred Data for the purposes set out in: Annex 1 Part A (Data Processing Table) of the Linked Agreement |
| | In both cases, any other purposes which are compatible with the purposes set out above.<br>☐ The purposes will update automatically if the information is updated in the Linked Agreement referred to.<br>☒<br>The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. |

**Table 4: Security Requirements**

| | |
|---|---|
| **Security of Transmission** | |
| **Security of Storage** | |
| **Security of Processing** | |

| | |
|---|---|
| **Organisational security measures** | |
| **Technical security minimum requirements** | TLS1.2+ with PFS (Perfect Forward Security), Encryption Rest, Encryption in Transit |
| **Updates to the Security Requirements** | ☐ The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.<br>☒ The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. |
| **TRANSFERS TO THE US,** | The Department for Science, Innovation and Technology (DSIT) Analysis of the UK Extension to the US-EU Data Bridge was issued in September 2023. The Information |

| | |
|---|---|
| **WHERE THE SUPPLIER HAS NOT SLEDCERTIFIED TO THE DATA PRIVACY FRAMEWORK (DPF)** | Commissioner's Office (ICO) have confirmed that the DSIT analysis offers adequate protections in relation to international data transfers to the US, where suppliers have not self-certified to the Data Privacy Framework.<br><br>HMRC is satisfied that the DSIT analysis concludes that US laws and practices provide adequate protections for people whose personal information is transferred to the US for risks to people's rights:<br><br>(i) arising in the US from third parties that are not bound by this IDTA accessing the transferred personal information in particular, government and public bodies; and<br><br>(ii) arising from difficulties enforcing the IDTA.<br><br>HMRC considers that it is reasonable and proportionate for it to rely on the DSIT analysis, given the scope of this assessment is as required under Article 45 UK GDPR, and the enactment of adequacy regulations under Section 17A DPA 2018 by the Secretary of State and Parliament, on the basis of that assessment.<br><br>HMRC will review this TRA if a new or amended version of the DSIT analysis is published, or the DSIT analysis is withdrawn. |

## Part 2: Extra Protection Clauses

| | |
|---|---|
| **Extra Protection Clauses:** | |
| **(i) Extra technical security protections** | |

| | |
|---|---|
| **(ii) Extra organisational protections** | |
| **(iii) Extra contractual protections** | |

# Part 3: Commercial Clauses

| | |
|---|---|
| **Commercial Clauses** | Commercial Clauses are not used |

# Part 4: Mandatory Clauses

## Information that helps you to understand this IDTA

### 1. This IDTA and Linked Agreements

1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.

1.2 This IDTA is made up of:

1.2.1 Part one: Tables;

1.2.2 Part two: Extra Protection Clauses; 1.2.3

Part three: Commercial Clauses; and

1.2.4 Part four: Mandatory Clauses.

1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.

1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).

1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

## 2. Legal Meaning of Words

2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.

2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

## 3. You have provided all the information required

3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.

3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:

3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and

3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.

3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

## 4. How to sign the IDTA

4.1 The Parties may choose to each sign (or execute):

4.1.1 the same copy of this IDTA;

4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;

4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

## 5. Changing this IDTA

5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:

5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the crossreference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;

5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;

5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or

5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.4 From time to time, the ICO may publish a revised Approved IDTA which:

5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

## 6. Understanding this IDTA

6.1 This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.

6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.

6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.

6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.

6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.

6.7 If there is any inconsistency or conflict between this IDTA and a Linked

Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.

6.8 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.

6.9 References to:

6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;

6.9.2 legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and

6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

### 7. Which laws apply to this IDTA

7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

## How this IDTA provides Appropriate Safeguards

### 8. The Appropriate Safeguards

8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:

8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and

8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.

8.2 The Exporter must:

8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and

8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.

8.3 The Importer must:

8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");

8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;

8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and

8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.

8.4 The Importer must ensure that at the Start Date and during the Term:

8.4.1 the Importer Information is accurate;

8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.

8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

## 9. Reviews to ensure the Appropriate Safeguards continue

9.1 Each Party must:

9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date

and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and

9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.

9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:

9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;

9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and

9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

## 10. The ICO

10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.

10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.

10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

## The Exporter

### 11. Exporter's obligations

11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.

11.2 The Exporter must:

11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and

11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.

11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.

11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

## The Importer

### 12. General Importer obligations

12.1 The Importer must:

12.1.1 only Process the Transferred Data for the Purpose;

12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;

12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;

12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;

12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and

12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).

12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

## 13. Importer's obligations if it is subject to the UK Data Protection Laws

13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and


OFFICIAL

- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

## 14. Importer's obligations to comply with key data protection principles

14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.

14.2 The Importer must:

14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

## 15. What happens if there is an Importer Personal Data Breach

15.1 If there is an Importer Personal Data Breach, the Importer must:

15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in cooperation with the Exporter and any Third Party Controller; and

15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:

15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.2.1.1 a description of the nature of the Importer Personal Data Breach;

15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.2.1.3 likely consequences of the Importer Personal Data Breach;

15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.2.1.5 contact point for more information; and

15.2.1.6 any other information reasonably requested by the Exporter,

15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.

15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.3.1 a description of the nature of the Importer Personal Data Breach;

15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.3.3 likely consequences of the Importer Personal Data Breach;

15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.3.5 contact point for more information; and

15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.

15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to

ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

## 16. Transferring on the Transferred Data

16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:

16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or

16.1.2 the third party has been added to this IDTA as a Party; or

16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or

16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or

16.1.5 the transfer is to the UK or an Adequate Country.

16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

### 17. Importer's responsibility if it authorises others to perform its obligations

17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).

17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.

17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.

17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has subcontracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references

to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

## What rights do individuals have?

### 18. The right to a copy of the IDTA

18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:

18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;

18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;

18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

## 19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

## 20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

20.4.1 Without Undue Delay (and in any event within one month);


OFFICIAL

20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

20.4.3 in clear and plain English that is easy to understand; and

20.4.4 in an easily accessible form together

with

20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and

20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.

20.5 If a Relevant Data Subject requests, the Importer must:

20.5.1 rectify inaccurate or incomplete Transferred Data;

20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;

20.5.3 cease using it for direct marketing purposes; and

20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.

20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:

20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or

20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or

20.6.3 the Extra Protection Clauses provide safeguards for the DecisionMaking which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.

### 21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor

21.1 Where the Importer is the Exporter's Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.

### 22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws

22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:

22.1.1 it is unable to reasonably verify the identity of an individual making the request; or

22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or

22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

## How to give third parties access to Transferred Data under Local Laws

### 23. Access requests and direct access

23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.

23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.

23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.

23.4 In so far as Local Laws allow, the Importer must:

23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and

23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

## 24. Giving notice

24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.

24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving

Party's next normal business day, and provided no notice of non-delivery or bounceback is received.

24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

## 25. General clauses

25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:

25.1.1 contain all the terms and conditions agreed by the Parties; and

25.1.2 override all previous contacts and arrangements, whether oral or in writing.

25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party

confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.

25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.

25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.

25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.

25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.

25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.

25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:

25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;

25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and

25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

## What happens if there is a breach of this IDTA?

### 26. Breaches of this IDTA

26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:

26.1.1 has breached this IDTA; or

26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.

26.2 In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

**27. Breaches of this IDTA by the Importer**

27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.

27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:

27.2.1 the Exporter must suspend sending Transferred Data to the Importer;

27.2.2 If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and

27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:

27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and

27.2.3.2 if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).

27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.

**28. Breaches of this IDTA by the Exporter**

28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful

Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.

28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.

28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

## Ending the IDTA

### 29. How to end this IDTA without there being a breach

29.1 The IDTA will end:

29.1.1 at the end of the Term stated in Table 2: Transfer Details; or

29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;

29.1.3 at any time that the Parties agree in writing that it will end; or

29.1.4 at the time set out in Section 29.2.

29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

29.2.1 its direct costs of performing its obligations under the IDTA; and/or

29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved IDTA.

### 30. How to end this IDTA if there is a breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and

30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or

30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;

30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

## 31. What must the Parties do when the IDTA ends?

31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and

31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.

31.2 When this IDTA ends (no matter what the reason is):

31.2.1 the Exporter must stop sending Transferred Data to the Importer; and

31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;

31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.

31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 2** (Legal Meaning of Words);
- **Section 6** (Understanding this IDTA);
- **Section 7** (Which laws apply to this IDTA);
- **Section 10** (The ICO);
- Sections 11.1 and 11.4 (Exporter's obligations);
- Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and
- **Section 36** (Legal Glossary).

## How to bring a legal claim under this IDTA

## 32. Your liability

32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.

32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

32.2.1 Party One's breach of this IDTA; and/or

32.2.2 where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.

32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

## 33. How Relevant Data Subjects and the ICO may bring legal claims

33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (The Appropriate Safeguards);
- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);

- **Section 11** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);
- **Section 19** (The Importer's contact details for the Relevant Data Subjects);
- **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
- **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or SubProcessor);
- **Section 23** (Access Requests and Direct Access);
- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);
- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.

33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).

33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).

33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.

33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

## 34. Courts legal claims can be brought in

34.1 The courts of the UK country set out in Table 2: Transfer Details have nonexclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).

34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details

34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including noncontractual claims) in any court in any country with jurisdiction to hear the claim.

34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

## 35. Arbitration

35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.

35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.

35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.

35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.

35.5 The English language must be used in the arbitral proceedings.

35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

## 36. Legal Glossary

| **Word or Phrase** | **Legal definition**<br>**(this is how this word or phrase must be interpreted in the IDTA)** |
|---|---|
| Access Request | As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data. |
| Adequate Country | A third country, or:<br>• a territory;<br>• one or more sectors or organisations within a third country;<br>• an international organisation; which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018. |

| | |
|---|---|
| Appropriate Safeguards | The standard of protection over the Transferred Data and of the Relevant Data Subject's rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| Approved IDTA | The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection |

| **Word or Phrase** | **Legal definition (this is how this word or phrase must be interpreted in the IDTA)** |
|---|---|
| | Act 2018 on 2 February 2022, as it is revised under Section 5.4. |
| Commercial Clauses | The commercial clauses set out in Part three. |
| Controller | As defined in the UK GDPR. |
| Damage | All material and non-material loss and damage. |
| Data Subject | As defined in the UK GDPR. |
| Decision-Making | As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data. |
| Direct Access | As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware. |

| | |
|---|---|
| Exporter | The exporter identified in Table 1: Parties & Signature. |
| Extra Protection Clauses | The clauses set out in Part two: Extra Protection Clauses. |
| ICO | The Information Commissioner. |
| Importer | The importer identified in Table 1: Parties & Signature. |
| Importer Data Subject Contact | The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19. |

| **Word or Phrase** | **Legal definition (this is how this word or phrase must be interpreted in the IDTA)** |
|---|---|
| Importer Information | As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA. |
| Importer Personal Data Breach | A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer. |
| Linked Agreement | The linked agreements set out in Table 2: Transfer Details (if any). |

| | |
|---|---|
| Local Laws | Laws which are not the laws of the UK and which bind the Importer. |
| Mandatory Clauses | Part four: Mandatory Clauses of this IDTA. |
| Notice Period | As set out in Table 2: Transfer Details. |
| Party/Parties | The parties to this IDTA as set out in Table 1: Parties & Signature. |
| Personal Data | As defined in the UK GDPR. |
| Personal Data Breach | As defined in the UK GDPR. |
| Processing | As defined in the UK GDPR.<br>When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf. |

| **Word or Phrase** | **Legal definition (this is how this word or phrase must be interpreted in the IDTA)** |
|---|---|
| Processor | As defined in the UK GDPR. |

| | |
|---|---|
| Purpose | The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to. |
| Relevant Data Subject | A Data Subject of the Transferred Data. |
| Restricted Transfer | A transfer which is covered by Chapter V of the UK GDPR |
| Review Dates | The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA. |
| Significant Harmful Impact | As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party. |
| Special Category Data | As described in the UK GDPR, together with criminal conviction or criminal offence data. |
| Start Date | As set out in Table 1: Parties and signature. |
| Sub-Processor | A Processor appointed by another Processor to Process Personal Data on its behalf.<br>This includes Sub-Processors of any level, for example a Sub-Sub-Processor. |
| Tables | The Tables set out in Part one of this IDTA. |

| Word or Phrase | Legal definition<br>(this is how this word or phrase must be interpreted in the IDTA) |
|---|---|
| Term | As set out in Table 2: Transfer Details. |
| Third Party Controller | The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor<br>If there is not a Third Party Controller this can be disregarded. |
| Transfer Risk Assessment or TRA | A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards |
| Transferred Data | Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details |
| UK Data Protection Laws | All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018. |
| UK GDPR | As defined in Section 3 of the Data Protection Act 2018. |
| Without Undue Delay | Without undue delay, as that phase is interpreted in the UK GDPR. |

## Alternative Part 4 Mandatory Clauses:

| | |
|---|---|
| **Mandatory Clauses** | Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses. |


OFFICIAL

# XI. Schedule 16- Buyer Security Buyer-Led Assurance

# Schedule 16 (Security)
# Buyer-led Assurance

# 1 Buyer Options

Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

| | | |
|---|---|---|
| **Buyer Security Policies** (see Paragraph 5) | | |
| The Buyer and Supplier acknowledge and agree that the existing main agreement, including Schedule 16, meets the material requirements set out in the identified policies relating to security management agreed standards herein. However, should Buyer during the term of the main agreement determine in good faith that any aspect of such policies satisfies all of the following three conditions: (i) relates to Supplier's delivery of Services within Buyer's own systems, (ii) is material to the relationship between Buyer and Supplier, and (iii) is not already covered by the main agreement, then Buyer may provide written notice to Supplier, and the parties shall negotiate in good faith a mutually acceptable amendment to the main agreement. | | X |
| **Locations** (see Paragraph 1 of the Security Requirements) | | |
| The Supplier and Subcontractors may store, access or Handle Government Data in: | the United Kingdom only | ☐ |
| | any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State) | ☐ |
| | anywhere in the world not prohibited by the Buyer, operating a risk-based approach | X |
| **Support Locations** (see Paragraph 1 of the Security Requirements) | | |
| The Supplier and Subcontractors may operate Support Locations in: | the United Kingdom only | ☐ |
| | any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State) | ☐ |
| | anywhere in the world not prohibited by the Buyer, operating a risk-based approach | X |

| | | |
|---|---|---|
| **Development Activity** (see Appendix 2) | | |
| The Buyer requires the Supplier to undertake Development Activity under this Contract and, as a consequence, Appendix 2 applies | | X |
| **Locations for Development Activity** (applies only if the option relating to Development Activities is selected; see Paragraph 1 of the Security Requirements) | | |
| The Supplier and Subcontractors may undertake Development Activity in: | the United Kingdom only | X |
| | any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State) | □ |
| | anywhere in the world not prohibited by the Buyer | □ |

## 2 Definitions

**Anti-virus Software** means software that:

(a) protects the Supplier Information Management System from the possible introduction of Malicious Software;

(b) scans for and identifies possible Malicious Software in the Supplier Information Management System;

(c) if Malicious Software is detected in the Supplier Information Management System, so far as possible:

(i) prevents the harmful effects of the Malicious Software; and

(ii) removes the Malicious Software from the Supplier Information Management System.

**Assets** means all assets and rights used by the Supplier to provide the Services in accordance with this Contract but excluding the Buyer Assets.

**Buyer--led Assurance** means the assessment of the Supplier Information Management System in accordance with Paragraph 15 by the Buyer or an independent information risk manager or other qualified professional appointed by the Buyer.

**Buyer Equipment** means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System.

**Backup and Recovery Plan** Supplier's Backup and Recovery procedures.

| | |
|---|---|
| **Breach Action Plan** | means a plan prepared under Paragraph 16.3 of the Security Requirements addressing any Breach of Security. |
| **Breach of Security** | means the occurrence of:<br>(a) any unauthorised access to or use of the Services,, the Sites, and/or any information or data used by the Buyer, the Supplier or any Subcontractor in connection with this Contract, including the Government Data and the Code;<br>(b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Subcontractor in connection with this Contract, including the Government Data and the Code; and/or<br>(c)<br>(d) the installation of Malicious Software in the:<br>(i)<br>(ii) Developed System;<br>(e)<br>(f) includes attempts to undertake the activities listed in sub-paragraph (a) where an investigation is warranted, and through such investigation, the Supplier has reasonable grounds to suspect that attempt: was part of a wider effort to specifically access information and communications technology operated by or on behalf of Central Government Bodies; or was undertaken, or directed by, a state other than the United Kingdom to specifically access information and communications technology operated by or on behalf of Central Government Bodies. |
| **Certification Requirements** | means the requirements set out in Paragraph 13.3. |
| **CHECK Scheme** | means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks. |
| **CHECK Service Provider** | means a company which, under the CHECK Scheme:<br>(a) has been certified by the National Cyber Security Centre;<br>(b) holds "Green Light" status; and<br>(c) is authorised to provide the IT Health Check services required by Paragraph 12 of the Security Requirements. |
| **CHECK Team Leader** | means an individual with a CHECK Scheme team leader qualification issued by the NCSC. |
| **CHECK Team Member** | means an individual with a CHECK Scheme team member qualification issued by the NCSC. |
| **Code** | means, in respect of the Developed System: |

(a) the source code;

(b) the object code;

(c) third-party components, including third-party coding frameworks and libraries; and (d) all supporting documentation.

| | |
|---|---|
| **Code Review** | means a periodic review of the Code by manual or automated means to:<br>(a) identify and fix any bugs; and<br>(a) ensure the Code complies with<br>(i) the requirements of this Schedule 16 (Security); and<br>(ii) the Secure Development Guidance. |
| **Code Review Plan** | means the document agreed with the Buyer under Paragraph 5.2 of the Security Requirements for Development setting out the requirements for, and frequency of, Code Reviews. |
| **Code Review Report** | means a report setting out the findings of a Code Review. |
| **Cyber Essentials** | means the Cyber Essentials certificate issued under the Cyber Essentials Scheme. |
| **Cyber Essentials Plus** | means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme. |
| **Cyber Essentials Scheme** | means the Cyber Essentials scheme operated by the National Cyber Security Centre. |
| **Data Migration Plan** | means the plan for the migration of the Government Data to the Buyer and/or the Replacement Supplier (as required by the Buyer) required by Paragraph 17 of the Security Requirements. |
| **Developed System** | means the software or system that the Supplier is required to develop under this Contract; Not applicable to this contract |
| **Development Activity** | means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including:<br>(a) coding; (b) testing;<br>(c) code storage; and (d) deployment. |
| **Development Environment** | means any information and communications technology system and the Sites that the Supplier or its Subcontractors will use to provide the Development Activity. |
| **EEA** | means the European Economic Area. |

| | |
|---|---|
| **End--user Device** | means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device provided by the Supplier or a Subcontractor and used in the provision of the Services. |
| **Email Service** | means a service that will send, or can be used to send, emails from the Buyer's email address or otherwise on behalf of the Buyer. |
| **Expected Behaviours** | means the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of https://www.gov.uk/government/publications/governmentsecurity-classifications/guidance-11-working-at-official-html |
| **Government Data Register** | means the register of all Government Data the Supplier, or any Subcontractor, receives from or creates for the Buyer, produced and maintained in accordance with Paragraph 18 of the Security Requirements. |
| **Government Security Classification Policy** | means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications |
| **Handle** | means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data. |
| **Higher-risk Subcontractor** | means a Subcontractor that Handles Government Data, where that data includes either:<br>(e) the Personal Data of 1000 or more individuals in aggregate during the period between the Start Date and the End Date; or<br>(a) any part of that Personal Data includes any of the following:<br>(i) financial information (including any tax and/or welfare information) relating to any person;<br>(ii) any information relating to actual or alleged criminal offences (including criminal records);<br>(iii) any information relating to children and/or vulnerable persons;<br>(iv) any information relating to social care;<br>(v) any information relating to a person's current or past employment; or<br>(vi) Special Category Personal Data; or |

| | |
|---|---|
| | (b) the Buyer in its discretion, designates a Subcontractor as a Higher- risk Subcontractor:<br>(i) in any procurement document related to this Contract; or<br>(ii) during the Term. |
| **HMG Baseline Personnel Security Standard** | means the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (https://www.gov.uk/government/publications/governmentbaseline-personnel-security-standard), as that document is updated from time to time. |
| **Independent Security Adviser** | means the independent and appropriately qualified and experienced security architect or expert appointed under Paragraph 20. |
| **ISO Certification** | means either of the following certifications:<br>(a) ISO/IEC27001:2013, where the certification was obtained before November 2022, but only until November 2025; and<br>(b) ISO/IEC27001:2022 in all other cases. |
| **IT Health Check** | means testing of the Supplier Information Management System by a CHECK Service Provider. |
| **Key Subcontractor Default** | has the meaning set out in Paragraph 10.5. |
| **Medium-risk Subcontractor** | means a Subcontractor that Handles Government Data, where that data<br>(a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Start Dateand the End Date; and (b) does not include Special Category Personal Data. |
| **Modules Register** | means the register of Third--party Software Modules required by Paragraph 7.3 of the Security Requirements. |
| **NCSC** | means the National Cyber Security Centre or any replacement or successor body carrying out the same function. |
| **NCSC Cloud Security Principles** | means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud/thecloud-security-principles. |
| **NCSC Device Guidance** | means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance. |

| | |
|---|---|
| **NCSC Protecting Bulk Personal Data Guidance** | means the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personaldata. |
| **NCSC Secure Design Principles** | means the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-designprinciples/cyber-security-design-principles. |
| **OWASP** | means the Open Web Application Security Project Foundation. |
| **OWASP Secure Coding Practice** | means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-codingpractices-quick-reference-guide/. |
| **OWASP Top Ten** | means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www-project-top-ten/. |
| **Privileged User** | means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges. |
| **Prohibited Activity** | means the storage, access or Handling of Government Data prohibited by a Prohibition Notice. |
| **Prohibition Notice** | means a notice issued under Paragraph 1.11 of the Security Requirements. |
| **Protective Monitoring System** | means the system implemented by the Supplier and its Subcontractors under Paragraph 14.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Government Data and the Code. |
| **RAP Trigger** | means the occurrence of one of the events set out in Paragraph 19.1. |
| **Relevant Activities** | means those activities specified in Paragraph 1.1 of the Security Requirements. |
| **Relevant Certifications** | means:<br>(a) in the case of the Supplier, (i) either:<br>(A) an ISO Certification; or<br>(B)<br>(ii) Cyber Essentials or equivalent; |



OFFICIAL

| | |
|---|---|
| **Relevant Convictions** | means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify. |
| **Remediation Action Plan** | means the plan prepared by the Supplier in accordance with Paragraph 12.13 to 12.17, addressing the vulnerabilities and findings in a IT Health Check report. |
| **Remote Location** | means a location other than a Supplier's or a Subcontractor's Site. |
| **Remote Working** | means the provision or management of the Services by Supplier Staff from a location other than a Supplier's or a Subcontractor's Site. |
| **Remote Working Policy** | the policy prepared and approved under Paragraph 3.8 of the Security Requirements and forming part of the Security Management Plan under which Supplier Staff are permitted to undertake Remote Working. |
| **Required Changes Register** | means the register recording each of the changes that the Supplier proposes to the Supplier Information Management System or the Security Management Plan together with:<br>(a) the details of any approval of the change provided by the Buyer, including any conditions or limitations on that approval; and<br>(b) the date:<br>(i) the date by which the change it to be implemented; and<br>(ii) the date on which the change was implemented. |
| **Residual Risk Statement** | means a notice issued by the Buyer that<br>(a) sets out the information risks associated with using the Supplier Information Management System; and (b)<br>confirms that the Buyer:<br>(i) is satisfied that the identified risks have been adequately and appropriately addressed; and<br>(ii) that the residual risks are understood and accepted by the Buyer. |
| **Risk Management Approval Statement** | the statement issued by the Buyer under Paragraph 15.7 following the Buyer-led Assurance of the Supplier Information Management System. |
| **Secure by Design Principles** | means the Secure by Design Principles issued by the Cabinet Office, as updated or replaced from time-to-time, currently found at https://www.security.gov.uk/policy-andguidance/secure-by-design/principles/. |
| **Secure Development Guidance** | means the Supplier's secure coding policy required under its ISO27001 Relevant Certification. |

| | |
|---|---|
| **Secure Location** | has the meaning given to that term in Paragraph 2.1(a) of Appendix 1 (Security Requirements). |
| **Security Controls** | means the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of https://www.gov.uk/government/publications/governmentsecurity-classifications/guidance-15-considerations-for-securityadvisors-html |
| **Security Management Plan** | means the document prepared in accordance with the requirements of Paragraph 14 and in the format, and containing the information, specified in [**insert cross-reference to guidance**]. |
| **Security Requirements** | mean the security requirements in Appendix 1 to this Schedule 16 (Security *Management*). |
| **Security Requirements for Development** | means the security requirement Appendix 2 to this Schedule 16 (Security). |
| **Security Test** | means:<br>(a)<br>(b) a Supplier Security Test. |
| **Security Working Group** | means the Board established under Paragraph 8 |
| **SIMS Subcontractor** | means a Subcontractor designated by the Buyer that provides or operates the whole, or a substantial part, of the Supplier Information Management System. |
| **SMP Subcontractor** | means a Subcontractor with significant market power, such that:<br>(a) they will not contract other than on their own contractual terms; and (b) either:<br>(i) there are no other substitutable suppliers of the particular services other than SMP Subcontractors; or<br>(ii) the Subcontractor concerned has an effective monopoly on the provision of the Services. |
| **Statement of Information Risk Appetite** | means the statement provided by the Buyer under Paragraph 14.1 setting out:<br>(a) the nature and level of risk that the Supplier accepts from the operation of the Supplier Information Management System; and<br>(b) the specific legal and regulatory requirements with which the Supplier must comply when Handling Government Data. |
| **Subcontractor** | means, for the purposes of this Schedule 16 (Security) only, any individual or entity that:<br>(a) forms part of the supply chain of the Supplier; and |

| | |
|---|---|
| | (b) has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Government Data, and this definition shall apply to this Schedule 16 in place of the definition of Sub-Contractor in Schedule 1 *(Definitions).* |
| **Subcontractor Staff** | means:<br>(a) any individual engaged, directly or indirectly, or employed, by any Subcontractor; and<br>(b) engaged in or likely to be engaged in:<br>(i) the performance or management of the Services;<br>(ii) or the provision of facilities or services that are necessary for the provision of the Services. |
| **Subcontractors' Systems** | means the information and communications technology system used by a Subcontractor in implementing and performing the Services, including:<br>(a) the Software;<br>(b) the Supplier Equipment;<br>(c) configuration and management utilities;<br>(d) calibration and testing tools;<br>(e) and related cabling; but does not include the Buyer System. |
| **Support Location** | means a place or facility where or from which individuals may access or Handle the Code or the Government Data. |
| **Support Register** | means the register of all hardware and software used to provide the Services produced and maintained in accordance with Paragraph 5 of the Security Requirements. |
| **Third-party Software Module** | means any module, library or framework that:<br>(a) is not produced by the Supplier or a Subcontractor as part of the Development Activity; and (b) either:<br>(i) forms, or will form, part of the Code; or<br>(ii) is, or will be, accessed by the Developed System during its operation. |
| **Third-party Tool** | means any Software used by the Supplier by which the Code or the Government Data is accessed, analysed or modified, or some form of operation is performed on it. |
| **UKAS** | means the United Kingdom Accreditation Service. |

| | |
|---|---|
| **UKAS-recognised Certification Body** | means:<br>(c) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or<br>(d) an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment. |
| **Wider Information Management System** | means<br>(a) any:<br>(i) information assets,<br>(ii) IT systems,<br>(iii) IT services; or Sites<br>that the Supplier or any Subcontractor will use to Handle, or support the Handling of, Government Data and provide, manage or support the provision of, the Services; and<br>(b) the associated information management system, including all relevant:<br>(i)<br>(ii) controls,<br>(iii) policies,<br>(iv) practices,<br>(v) procedures,<br>(vi) processes; and<br>(vii) |

## 3 Introduction

This Schedule 16 (Security) sets out:

3.1 the Buyer's decision on where the Supplier may:

(a) store, access or Handle Government Data;

(b) undertake the Development Activity;

(c) host the Development Environment; and

(d) locate Support Locations,

(in Paragraph 1);

3.2 the principles of security that apply to this Contract (in Paragraph 4);

3.3 the requirement to obtain a Risk Management Approval Statement (in Paragraphs 6 and 15);

3.4 the annual confirmation of compliance to be provided by the Supplier (in Paragraph 7);

3.5 the governance arrangements for security matters, where these are not otherwise specified in Schedule 13 (Contract Management) (in Paragraph 8);

3.6 access to staff (in Paragraph 9);

3.7 obligations in relation to Subcontractors (in Paragraph 10);

3.8 the responsibility of the Buyer to determine the Supplier Information Management System that will be subject to Buyer-led Assurance (in Paragraph 11);

3.9 the Certification Requirements (in Paragraph 13);

3.10 the development, monitoring and updating of the Security Management Plan by the Supplier; or (in Paragraphs 14, 16 and 17);

3.11 the granting by the Buyer of approval for the Supplier to commence:

(a) the provision of Operational Services; and/or

(b) Handling Government Data (in Paragraph 15);

3.12 the management of changes to the Supplier Information Management System (in Paragraph 18); and

3.13 the Buyer's additional remedies for breach of this Schedule 16 (Security), including:

(a) the requirement for Remediation Action Plans (in Paragraph 19); (b)

the appointment of Independent Security Advisers (in Paragraph 20); and (c)

the withholding of Charges by the Buyer (in Paragraph 21).

## 4 Principles of security

4.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Government Data and, consequently, on the security of:

(a) the Buyer System;

(b) the Supplier System;

(c) the Sites;

(d) the Services; and

(e) the Supplier Information Management System.

4.2 The Parties shall share information and act in a co-operative manner at all times to further the principles of security in Paragraph 4.1.

4.3 Notwithstanding the involvement of the Buyer in the Buyer-led Assurance of the Supplier Information Management System, the Supplier remains responsible for:

(a) the security, confidentiality, integrity and availability of the Government Data when that Government Data is under the control of the Supplier or any of its Subcontractors; and

## 5 Security requirements

5.1 The Supplier must, unless otherwise agreed in writing with the Buyer:

(a) comply with the Security Requirements in Appendix 1;

(b) where the relevant option in Paragraph 1 is selected, comply with the Security Requirements for Development in Appendix 2;

(c) where the relevant option in Paragraph 1 is selected, comply with the Buyer Security Policies; and

(d) ensure that Subcontractors comply with substantially similar requirements as outlined in this document:

(i)

5.2 Where the Buyer selects the option in Paragraph 1 requiring the Supplier to comply with the Buyer Security Policies, if there is an inconsistency between the Buyer Security Requirements and the requirement of this Schedule 16 (Security), then the requirements of this Schedule will prevail to the extent of that inconsistency.

## 6 Buyer to proceed

Notwithstanding anything in this Contract, the Supplier may not:

6.1 commence the provision of any Operational Services; or

6.2 Handle any Government Data,

unless

6.3 the Supplier has obtained the Relevant Certifications under Paragraph 13;

6.4 Intentionally omitted

6.5 Intentionally omitted

## 7 Supplier confirmation

7.1 The Supplier will, on an annual basis or on the event of a material change or in the identification of a critical vulnerability or risk, make available to Buyer a copy of its SOC2 report and additional security collateral via its Trust Center for Buyer's review and understanding of Supplier's control status.

## 8 Intentionally omitted

## 9 Staff

9.1 The Supplier must ensure that at all times it maintains within the Supplier Staff sufficient numbers of qualified, skilled security professionals to ensure the Supplier complies with the requirements of this Schedule 16 (Security).

9.2 The Supplier must appoint:

(a) a senior individual within its organisation with accountability for managing security risks and the Supplier's implementation of the requirements of this Schedule 16 (Security); and

(b) a senior individual within the team responsible for the delivery of the Services

9.3 The individuals appointed under Paragraph 9.2:

(a) must have sufficient experience, knowledge to undertake their roles effectively

(b)

9.4 Intentionally omitted

9.5 Intentionally omitted

## 10 Intentionally omitted

## 11 Intentionally omitted

## 12 Government Data Handled using Supplier Information Management System

12.1 The Supplier acknowledges that it:

(a) is intended only for the Handling of Government Data that is classified as OFFICIAL; and

(b) is not intended for the Handling of Government Data that is classified as OFFICIAL SENSITIVE or SECRET or TOP SECRET,

in each case using the Government Security Classification Policy.

12.2 The Supplier must:

(a) not alter the classification of any Government Data; and

(b) if it becomes aware that any Government Data classified as OFFICIAL SENSITIVE SECRET or TOP SECRET is being Handled using the Supplier Information Management System:

(i) immediately inform the Buyer; and

(ii) follow any reasonable instructions from the Buyer concerning that Government Data.

12.3 Intentionally omitted

## 13 Certification Requirements

13.1 The Supplier shall ensure that:

(a) it; is certified as compliant with the Relevant Certifications, that is to say:

(b) in the case of the Supplier,:

(ii) either:

(A) an ISO 27001 Certification; or

(B) SOC 2

(i) Cyber Essentials;

(or equivalent);

13.2 Unless otherwise agreed by the Buyer, before it begins to provide the Services, the Supplier must provide the Buyer with a copy of:

(a) the Relevant Certifications for it; and

(b) the relevant scope and statement of applicability required under the ISO/IEC 27001 Relevant Certifications.

13.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications for it are:

(a) currently in effect;

(b) Intentionally omitted

(c) are not subject to any condition that may impact the provision of the Services or the Development Activity (**Certification Requirements**).

13.4 The Supplier must make available through the Supplier's Trust Center updated certification materials and provide notifications that Buyer can subscribe to.

13.5 Intentionally omitted

## 14 Intentionally omitted

## 15 Intentionally omitted

## 16 Remediation Action Plan

16.1 Intentionally omitted

16.2 Where non-compliance with section 13 above is identified, the supplier must track and manage remediation in line with their internal processes. This must include full details of that issue, proof of remediation and date of remediation.

## 17 Intentionally omitted



OFFICIAL

# Appendix 1 Security Requirements

## 1 Location

**Location for Relevant Activities**

1.1 Unless otherwise agreed with the Buyer, the Supplier must, at all times:

(a) provide the Services;

(b) intentionally omitted

(c) store, access or Handle Government Data;

(d) intentionally omitted

(e) intentionally omitted (together, the **Relevant Activities**) only in or from the geographic areas permitted by the Buyer in Paragraph 1.

1.2 Where the Buyer has not selected an option concerning location in Paragraph 1, the Supplier may only undertake the Relevant Activities in or from:

(a) the United Kingdom; or

(b) a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

1.3 The Supplier must, undertake the Relevant Activities in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier ;

(b) that binding agreement includes obligations on the entity in relation to security management equivalent to those imposed on Subcontractors in this Schedule 16 (Security);

(c) the Supplier has taken reasonable steps to assure itself that the entity complies with the binding agreement;

1.4

(a) the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and

(b) if the Buyer does not grant permission to use that location or those locations, the Supplier must, within such period as the Buyer may specify:

(i) cease to store, access or Handle Government Data at that location or those locations;

(ii) intentionally omitted

**Support Locations**

1.5 Intentionally omitted

1.6 Intentionally omitted

1.7 Intentionally omitted

**Third--party Tools**

1.8 Before using any Third-party Tool, the Supplier must,:

(a) perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Tool;

(b) intentionally omitted

1.9 Intentionally omitted.

1.10 Intentionally omitted

## 2 Physical Security

2.1 The Supplier must ensure, ensure, that:

(a) all Sites, locations at which Relevant Activities are performed, or Support Locations (**Secure Locations**) have the necessary physical protective security measures in place to prevent unauthorised access, damage and interference, whether malicious or otherwise, to Government Data;

2.2 Intentionally omitted

## 3 Vetting, Training and Staff Access

**Vetting before performing or managing Services**

3.1 The Supplier must not engage Supplier Staff, in:

(a) any activity relating to the provision or management of the Services; or

(b) any activity that allows or requires the Handling of Government Data,

unless:

(c) that individual has passed the Supplier's background check and screening process

(d) Intentionally omitted

3.2 As a minimum, Supplier Personnel, must have completed the Supplier's background check and screening process in line with the Baseline Personnel Security Standard (BPSS) or materially equivalent to, subject to applicable local laws. Any additional vetting requirements for Supplier Staff involved in the delivery of

professional services to the Buyer, will be determined by the Authority on a case-by-case basis and set out in a mutually agreed SOW.

(a) The checks required for the HMG Baseline Personnel Security Standard (BPSS) or equivalent PreEmployment Checks are:

(i) The individual's identity;

(ii) where that individual will work in; and if the individual works within the United Kingdom,

(A) that individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;

(iii) the individual's previous employment history; and

(iv) that the individual has no Relevant Convictions;

3.3 Intentionally omitted

**Annual training**

3.4 The Supplier must ensure, that all Supplier Staff, complete and pass security training at least once every calendar year that covers:

(a) general training concerning security and data handling;

(b) Phishing, including the dangers from ransomware and other malware; and

(c) Intentionally omitted

**Staff access**

3.5 The Supplier must ensure, that individual Supplier Staff can access only the Government Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

3.6 The Supplier must ensure, that where individual Supplier Staff no longer require access to the Government Data or any part of the Government Data, their access to the Government Data or that part of the Government Data is revoked immediately when their requirement to access Government Data ceases.

3.7 Where requested by the Buyer, the Supplier must remove, an individual Supplier Staff's access to the Government Data, or part of that Government Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request to the extent reasonable and feasible.

## 4 End-user Devices

4.1 The Supplier must manage, all End-user Devices on which Government Data or Code is stored or Handled in accordance the following requirements:

(a) the operating system and any applications that store, Handle or have access to Government Data or Code must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Government Data and Code must be encrypted

(d) the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;

(e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data and Code to ensure the security of that Government Data and Code;

(f) the Suppler can, without physical access to the End-user Device, remove or make inaccessible all Government Data or Code stored on the device and prevent any user or group of users from accessing the device;

(g) all End-user Devices are within the scope of any Relevant Certification.

4.2 Intentionally omitted

4.3 Intentionally omitted

## 5 Hardware and software support

5.1 Before using any software as part of the service offering the Supplier must:

(a) perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that software; and

(b) where there are any recognised security vulnerabilities, either:

(i) remedy vulnerabilities; or

(ii) ensure that the design of the Supplier's controls mitigates those vulnerabilities.

5.2 The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.

5.3 Intentionally omitted

## 6 Encryption

6.1 Intentionally omitted

6.2 Intentionally omitted

6.3 Unless Paragraph 6.4 applies, the Supplier must ensure, that Government Data is encrypted:

(a) when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

(b) when transmitted.

6.4 Where the Supplier, cannot encrypt Government Data as required by Paragraph 6.2, the Supplier must:

(a) immediately inform the Buyer of the subset or subsets of Government Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Supplier proposes to take to provide equivalent protection to the Buyer as encryption;

(c) provide the Buyer with such additional information relating to the information provided under Paragraphs (a) and (b) as the Buyer may reasonably require.

6.5 The Buyer, the Supplier shall meet to agree appropriate protective measures for the unencrypted Government Data.

6.6 Intentionally omitted

## 7 Backup and recovery of Government Data

**Backups and recovery of Government Data**

7.1 The Supplier must backup and recover the Government Data in accordance with the Backup and Recovery Plan to ensure the recovery point objective and recovery time objective in Paragraph 7.3(a).

7.2 Any backup system operated by the Supplier forms part of the Supplier System to which this Schedule 16 (Security) and the Security Requirements apply.

**Backup and Recovery Plan**

7.3 the Backup and Recovery Plan must provide for:

(a) in the case of a full or partial failure of the Supplier System:

(i) a recovery time objective of **8 hours**; and

(ii) a recovery point objective of **4 hours**; and

(b) Intentionally omitted

7.4 In doing so, the Backup and Recovery Plan must ensure that in respect of any backup system operated by the Supplier:

(a) the backup location for Government Data is sufficiently physically and logically separate from the rest of the Supplier System that it is not affected by any Disaster affecting the rest of the Supplier System;

(b) there is sufficient storage volume for the amount of Government Data to be backed up;

(c) all back-up media for Government Data is used in accordance with the manufacturer's usage recommendations;

(d) newer backups of Government Data do not overwrite existing backups made during the retention period specified in Paragraph 7.3(a)(ii);

(e) the backup system monitors backups of Government Data to:

(i) identifies any backup failure; and

(ii) confirm the integrity of the Government Data backed up;

(f) any backup failure is remedied promptly;

(g) the backup system monitors the recovery of Government Data to:

(i) identify any recovery failure;

(ii) confirm the integrity of Government Data recovered; and

(h) any recovery failure is promptly remedied.

## 8 Email

8.1 Buyer has the option to setup their own SMTP service for the GitLab Dedicated service offering. Details can be found at https://docs.gitlab.com/subscriptions/gitlab_dedicated/#email-service.

## 9 DNS

Intentionally omitted

## 10 Malicious Software

10.1 The Supplier shall install and maintain Anti-virus Software or equivalent technologies on its production systems and user endpoints.

10.2 The Supplier must ensure that such Anti-virus Software:

(a) prevents the installation of the most common forms of Malicious Software;

(b) is configured to perform automatic software and definition updates;

(c) intentionally omitted

(d) performs regular scans of the systems to check for and prevent the introduction of Malicious Software; and

(e) where Malicious Software has been introduced into the Supplier's systems, identifies, contains the spread of, and minimises the impact of Malicious Software.

10.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

10.4 Intentionally omitted

## 11 Vulnerabilities

11.1 Unless the Buyer otherwise agrees, the Supplier must ensure that it applies security patches to vulnerabilities in accordance with its vulnerability management standard, and no later than:

(a) 30 days after the public release of patches for vulnerabilities classified as "critical";

(b) 30 days after the public release of patches for vulnerabilities classified as "high"; and

(c) 90 days after the public release of patches for vulnerabilities classified as "medium".

11.2 The Supplier must:

(a) scan the Supplier's environment at least once every month to identify any unpatched vulnerabilities; and

(b) if the scan identifies any unpatched vulnerabilities ensure they are patched in accordance with Paragraph 11.1.

11.3 For the purposes of this Paragraph 11, the Supplier must implement a method for classifying vulnerabilities to its environment that is aligned to recognised vulnerability assessment systems, such as:

(a) the National Vulnerability Database's vulnerability security ratings; or

(b) Microsoft's security bulletin severity rating system.

## 12 Security testing

**Responsibility for security testing**

12.1 The Supplier is solely responsible for:

(a) the costs of conducting any security testing required by this Paragraph 12; and

(b) the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

**Security tests by Supplier**

12.2 The Supplier must:

(a) Intentionally omitted

(b) at least once during each Contract Year;

(c) undertake the following activities:

(d) conduct security testing of the Supplier's service offerings in accordance with Paragraph 12.8 to 12.10;

(e) Intentionally omitted

12.3 In addition to its obligations under Paragraph 12.2, the Supplier must undertake any tests required by:

(a) Intentionally omitted

(b) the ISO27001 Certification Requirements;

(c) intentionally omitted

12.4 The Supplier must:

(a) design and implement the Supplier Security Tests so as to minimise the impact on the delivery of the Services;

(b) intentionally omitted

12.5 Where the Supplier fully complies with Paragraph 12.4, if a Supplier Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be entitled to relief in respect of such Performance Failure for that Measurement Period.

12.6 The Supplier shall provide the Buyer with an executive summary report of such tests.

12.7 Intentionally omitted

**Remedying vulnerabilities**

12.8 In addition to complying with Paragraphs 12.13 to 12.21, the Supplier must remedy:

(a) Vulnerabilities discovered as a result of security tests in accordance with the timelines outlined in Supplier's vulnerability management standard and section 11.1 above.

(b) Intentionally omitted

(c) Intentionally omitted

## 13 Access Control

13.1 The Supplier must:

(a) identify and authenticate all persons who access its systems before they do so;

(b) require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;

(c) allow access only to those parts of its systems that those persons require; (d) maintain records detailing each person's access to its systems.

13.2 The Supplier must ensure, that the user accounts for Privileged Users of its systems:

(a) are allocated to a single, individual user;

(b) are accessible only from dedicated End--user Devices;

(c) Intentionally omitted

(d) automatically log the user out of its systems after a period of time that is proportionate to the risk environment during which the account is inactive; and

(e) are:

(i) restricted to a single role or small number of roles;

(ii) intentionally omitted

13.3 The Supplier must ensure that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for 20 Working Days before deletion.

13.4 The Supplier must require that Privileged Users use unique and substantially different high-complexity passwords for their different accounts on its systems.

13.5 The Supplier must:

(a) configure any hardware that forms part of its systems that is capable of requiring a password before it is accessed to require a password; and

(b) change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

## 14 Event logging and protective monitoring

**Protective Monitoring System**

14.1 The Supplier must implement an effective system of monitoring and reports, analysing access to and use of its systems, the Development Environment, the Government Data and the Code to:

(a) identify and prevent potential Breaches of Security;

(b) respond effectively and in a timely manner to Breaches of Security that do occur;

(c) identify and implement changes to its systems to prevent future Breaches of Security; and

(d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using its systems,

(**Protective Monitoring System**).

14.2 The Protective Monitoring System must provide for:

(a) event logs and audit records of access to its systems; and

(b) regular reports and alerts to identify:

(i) changing access trends;

(ii) unusual usage patterns; or

(iii) the access of greater than usual volumes of Government Data;

(c) the detection and prevention of any attack on its systems or the Development Environment using common cyber-attack techniques;

**Event logs**

14.3 .Intentionally omitted

(a) Intentionally omitted

(b) Intentionally omitted

## 15 Audit rights

**Right of audit**

15.1 The Buyer may undertake an audit of the Supplier to:

(a) verify the Supplier's compliance with the requirements of this Schedule 16 (Security) and the Data Protection Laws as they apply to Government Data;

(b) Such audits will be limited to the information contained in the Supplier's Trust Center, public handbook, and product documentation site.

15.2 Any audit undertaken under Paragraph 15.1:

(a) may only take place during the Term; and

(b) is in addition to any other rights of audit the Buyer has under this Contract.

15.3 The Buyer may not undertake more than one audit under Paragraph 15.1 in each calendar year unless the Buyer has reasonable grounds for believing:

(a) there has been a Breach of Security affecting the Government Data

**Conduct of audits**

15.4 The Buyer must use reasonable endeavours to provide 15 Working Days' notice of an audit.

15.5 The Buyer must when conducting an audit:

(a) comply with all relevant policies and guidelines of the Supplier concerning access to the provided information; and

(b) use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or delay the provision of the Services.

15.6 The Supplier must, provide the Buyer with all co-operation and assistance the Buyer may reasonably require, including:

(a) all information requested by the Buyer within the scope of the audit;

(b) access to the Supplier Staff.

**Response to audit findings**

15.7 Where an audit finds that:

(a) the Supplier has not complied with this Contract or the Data Protection Laws as they apply to the Government Data; or

(b) there has been a Security Breach affecting the Government Data

the Buyer may request the Supplier to remedy those findings at its own cost and expense and within the time reasonably specified by the Buyer. The Supplier will review and consider such requests in a reasonable timeframe.

15.8 The exercise by the Buyer of any rights it may have under this Paragraph 15 does not affect the exercise by it of any other or equivalent rights it may have under this Contract in respect of the audit findings.

## 16 Breach of Security

**Reporting Breach of Security**

16.1 If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 48 hours.

**Immediate steps**

16.2 The Supplier must, upon becoming aware of a Breach of Security immediately:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

(d) prevent a further Breach of Security in the future which exploits the same root cause failure;

**Subsequent action**

16.3 As soon as reasonably practicable and, in any event, within five Working Days of the occurrence of the Breach of Security provide to the Buyer: (a) full details of the Breach of Security; and

(b) if required by the Buyer:

(i) a root cause analysis; and

(ii) a plan addressing the Breach of Security,

(a **Breach Action Plan**).

16.4 The Breach Action Plan must set out:

(a) in respect of each issue identified in the root cause analysis:

(i) how the issue will be remedied;

(ii) the date by which the issue will be remedied; and

(iii) the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed;

(b) intentionally omitted

(c) the infrastructure, services and systems (including any contact centre facilities) the Supplier will establish to undertake the remediation, communication and engagement activities.

16.5 The Supplier shall promptly provide the Buyer with such technical and other information relating to the Breach Action Plan as the Buyer reasonably requests.

16.6 When implementing the Breach Action Plan, the Supplier must:

(a) establish infrastructure, services and systems referred to in the Breach Action Plan;

(b) communicate and engage with affected individuals in accordance with the Breach Action Plan;

(c) communicate and engage with the Buyer; and

(d) engage and deploy such additional resources as may be required to perform its responsibilities under the Breach Plan and this Contract in respect of the Personal Data Breach without any impact on the provision of the Services;

(e) intentionally omitted

16.7 The obligation to provide and implement a Breach Action Plan under Paragraphs 16.3 to 16.7 continues notwithstanding the expiry or termination of this Contract.

**Costs of preparing and implementing Breach Action Plan**

16.8 The Supplier is solely responsible for its costs in preparing and implementing a Breach Action Plan.

**Reporting of Breach of Security to regulator**

16.9 Where the Law requires the Supplier report a Breach of Security to the appropriate regulator, the Supplier must:

(a) make that report within the time limits:

(i) specified by the relevant regulator; or

(ii) otherwise required by Law;

(b) intentionally omitted

16.10 Where the Law requires the Buyer to report a Breach of Security to the appropriate regulator, the Supplier must:

(a) provide such information and other input as the Buyer reasonably requires and as required by Law within the timescales specified by the Buyer to the extent required by Law;

(b) ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Buyer.

## 17 Intentionally omitted

## 18 Return and deletion of Government Data

18.1 Intentionally omitted

18.2 The GitLab application is designed to allow customers to delete their own data when no longer needed. If Supplier's support is requested by the Buyer when deleting or transferring data, Supplier uses industry standard methodologies to securely dispose of data upon expiration of legal, regulatory, or contractual data retention obligations and to protect data during electronic transfer.

18.3 Buyer has access to their data stored in the GitLab platform through standard user and programmatic interfaces.

18.4 Intentionally omitted

# Appendix 2 Security Requirements for Development

## 1 Secure Software Development by Design

1.1 The Supplier must implement secure development and deployment practices to ensure that:

(a) no Malicious Software is introduced into the Developed System.

(b) Intentionally omitted

1.2 To those ends, the Supplier must:

(a) comply with the Secure Development Guidance to the extent required under ISO 27001; and (b)

intentionally omitted

1.3 In particular, the Supplier must:

(a) ensure that all Supplier Staff engaged in Development Activity are:

(i) trained and experienced in securecode development;

(ii) provided with regular training in secure software development and deployment;

(b) ensure that all Code:

(i) is subject to a clear, well -organised, logical and documented architecture;

(ii) follows OWASP Secure Coding Practice

(iii) follows recognised secure coding standard, where one is available;

(iv) employs consistent naming conventions;

(v) is coded in a consistent manner and style;

(vi) is clearly and adequately documented to set out the function of each section of code;

(vii) is subject to appropriate levels of review through automated and non-automated methods both as part of:

(A) any original coding; and (B)

at any time the Code is changed;

(c) ensure that all Development Environments:

(i) protect access credentials and secret keys;

(ii) is logically separate from all other environments, including production systems, operated by the Supplier;

(iii) requires multi-factor authentication to access;

(iv) have onward technical controls to protect the Developed System in the event a Development Environment is compromised; and

(v) use network architecture controls to constrain access from the Development Environment to the Developed System.

## 2 Secure Architecture

2.1 Intentionally omitted

2.2 Intentionally omitted

2.3 Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that the Developed System encrypts Government Data:

(a) when the Government Data is stored at any time when no operation is being performed on it; and

(b) when the Government Data is transmitted.

2.4 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in Paragraphs 13.1 to 13.4 of the Security Requirements.

## 3 Code Repository and Deployment Pipeline

The Supplier must:

3.1 Intentionally omitted

3.2 ensure user access to code repositories is authenticated using credentials, with passwords or private keys;

3.3 ensure secret credentials are separated from source code.

3.4 run automatic security testing as part of any deployment of the Developed System.

## 4 Development and Testing Data

The Supplier must, use only anonymised, dummy or synthetic data when using data within the Development Environment for the purposes of development and testing.

## 5 Code Reviews

5.1 The Supplier must: (a) regularly review the Code in accordance with the requirements of this

Paragraph 5 (**Code Review**).

5.2 Intentionally omitted

5.3 Intentionally omitted

5.4 Intentionally omitted

5.5 Intentionally omitted

5.6 Where the Code Review identifies any security vulnerabilities, the Supplier must:

(a) remedy these at its own cost and expense;

(b) ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and

(c) modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re-occur;

(d) Intentionally omitted

## 6 Third--party Software

Intentionally omitted

## 7 Third--party Software Modules

7.1 Where the Supplier incorporates a Third--party Software Module into the Code, the Supplier must:

(a) verify the source and integrity of the Third--party Software Module by cryptographic signing or such other measure that provides the same level of assurance;

(b) perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third--party Software Module;

(c) continue to monitor any such Third--party Software Module so as to ensure it promptly becomes aware of any newly -discovered security vulnerabilities;

(d) take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.

7.2 For the purposes of Paragraph 7.1(b), the Supplier must perform due diligence that is proportionate to the significance of the Third-party Software Module within the Code.

7.3 The Supplier must produce and maintain an SBOM of its dependencies that support the service offering.

**XII.**

# Schedule 1 (Performance Levels)

## Definitions

In this Schedule, the following words shall have the following meanings and they shall supplement the definitions in the order form.

| | |
|---|---|
| **"Critical KPI Failure"** | means a failure by the Supplier to achieve the specified Key Performance Indicators that constitutes a Material Breach of this Contract; |
| **"KPI Failure"** | a failure to meet the KPI Performance Measure in respect of a Key Performance Indicator; |
| **"KPI Performance Measure"** | shall be as set out against the relevant Key Performance Indicator in the Annex to Part A of this Schedule; |
| **"KPI Threshold"** | shall be as set out against the relevant Key Performance Indicator in the Annex to Part A of this Schedule; |
| **“Measurement Period”** | in relation to a Key Performance Indicator, the period over which the Supplier’s performance is measured as set out against the relevant Key Performance Indicator in the Annex to Part A of this Schedule; |

| | |
|---|---|
| | has the meaning given in Paragraph 1.2 of Part B of this Schedule; |
| **"Performance Monitoring Reports"** | |
| | has the meaning given in Paragraph 1.3 of Part B of this Schedule; |
| **"Performance Review Meetings"** | |
| | any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the |
| **"Service Credits"** | Buyer in respect of any failure by the Supplier to meet one or more Key Performance Indicators; and |
| | has the meaning given to it in the Award Form. |
| **"Service Credit Cap"** | |

**What happens if you don't meet the Key Performance Indicators**

The Supplier shall at all times provide the Deliverables to meet or exceed the KPI Performance Measure for each Key Performance Indicator.

The Supplier acknowledges that any KPI Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any KPI Performance Measure.

The Supplier shall send Performance Monitoring Reports to the Buyer, upon Buyer's request, detailing the level of service which was achieved in

accordance with the provisions of Part B (Performance Monitoring) of this Schedule to enable the Buyer to assess the Supplier's performance against each Key Performance Indicator in each Measurement Period.

A Service Credit shall be the Buyer's exclusive remedy for a KPI Failure except where:

the Supplier has over the previous twelve (12) Month period exceeded the Service Credit Cap in three consecutive months; and/or the

KPI Failure:

exceeds the relevant KPI Threshold provided that such failure constitutes a Material Breach;

has arisen due to a wilful Default by the Supplier; results in the corruption or loss of any Government Data provided that such failure constitutes a Material Breach and/or

the Buyer is also entitled to terminate this Contract for Material Breach

**Critical KPI Failure**

On the occurrence of a Critical KPI Failure that is not remedied within 30 days:

any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and the Buyer shall (subject to the

Service Credit Cap) be entitled to terminate the

Contract for Material Breach and Clause 11.5.1 shall apply (**"Consequences of Critical KPI Failure"**),

# Part A: Key Performance Indicators and Service Credits

**Key Performance Indicators**

If the level of performance of the Supplier:

fails to meet any KPI Performance Measure; or causes

a Critical KPI Failure to occur,

the Supplier shall promptly notify the Buyer in writing and the Buyer upon becoming aware of such failure, in its absolute discretion and without limiting any other of its rights, may:

require the Supplier to promptly use reasonable efforts to take remedial action that is reasonable to mitigate the impact on the Buyer and is intended to prevent a KPI Failure or Critical KPI Failure from taking place or recurring;

instruct the Supplier to provide a documented Rectification Plan; if a KPI Failure has occurred, deduct the applicable Service Credits payable by the Supplier to the Buyer in accordance with Appendix 2B of Special Terms 1; and/or if a Critical KPI Failure has occurred, exercise its right to Consequences of Critical KPI Failure.

**Service Credits**

The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

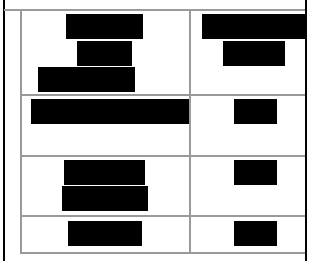
Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule and Appendix 2B of Special Terms 1.

# Annex to Part A: Key Performance Indicators and Service Credits Table

| Key Performance Indicators (KPIs) |
| --- |
| **KPI details** |

| Key Performance Indicator Performance Criterion | Key Indicator | KPI Performance Measure | KPI Threshold | Service Credit for each Service Period | Measurement Period |
|---|---|---|---|---|---|
| **KPI 1:** Support First Response Time SLA | Support First response time SLAs (as set out at https://about.gitlab.com/support/) to be as follows:<br>**Support Impact** / **First Response Time SLA**<br>Emergency (Your GitLab instance is completely unusable) — 30 minutes<br>Highly Degraded (Important features unavailable or extremely slow; No acceptable workaround) — 4 hours<br>Medium Impact — 8 hours<br>Low Impact — 24 hours | [redacted] of all support tickets within the Measurement Period provided first response within the Key Indicator times corresponding to its support impact category | [redacted] of all support tickets within the Measurement Period provided first response within the Key Indicator times corresponding to its support impact category | 0% | Measured at the end of each quarter of the Contract Year, Supplier will provide, upon request, a quarterly report of all support tickets opened, and indicate the number of tickets falling outside the KPI Threshold |

| Key Performance Indicators (KPIs) | | | | | |
|---|---|---|---|---|---|
| **KPI details** | | | | | |
| **Key Performance Indicator Performance Criterion** | **Key Indicator** | **KPI Performance Measure** | **KPI Threshold** | **Service Credit for each Service Period** | **Measurement Period** |

| | | | | | |
|---|---|---|---|---|---|
| **KPI 2**: Service Level Availability | "**Service Level Availability**" as set out in Appendix 2B of Special Terms 1 | 99.5% "Service Level Objective" as per Appendix 2B of Special Terms 1 | 90% | On a month-by-month basis, if Service Level Availability does not meet or exceed the SLO, a Downtime Credit of up to the percentages set out below of the Fees paid by the Buyer for that month will apply, calculated as set out in Appendix 2B of Special Terms 1.<br>  | Monthly |
| **KPI 3:** UK Carbon Offset Tree Planting KPI | 250 trees planted (via Supplier's selected vendor) each Contract Year | 100% | 80% | 0% | Measured at the end of each Contract Year |

The Service Credits shall be calculated in accordance with Appendix 2B of Special Terms 1:

1. Mapping of levels of performance under the KPI Performance Measures to ratings under regulation 39(5) of the Procurement Regulations 2024

| **Regulation 39(5) Rating** | **Level of performance against the KPI Performance Measure**<br>**KPI 1 Support First Response Time SLA** | **Level of performance against the KPI Performance Measure**<br>**KPI 2 SLA** | **Level of performance against the KPI Performance Measure**<br>**KPI 3 Tree Planting** |
|---|---|---|---|
| Good | KPI Performance Measure | KPI Performance Measure | KPI Performance Measure |
| Approaching Target | 89 to 90% | 98.0 to 99.5% | 95 to 99.9% |

| | | | |
|---|---|---|---|
| Requires Improvement | 80 to 88.9% | 90-97.9 % | 85 to 94.9% |

| **Regulation 39(5) Rating** | **Level of performance against the KPI Performance Measure**<br>**KPI 1 Support First Response Time SLA** | **Level of performance against the KPI Performance Measure**<br>**KPI 2 SLA** | **Level of performance against the KPI Performance Measure**<br>**KPI 3 Tree Planting** |
|---|---|---|---|
| Inadequate | Below KPI Threshold | Below KPI Threshold | Below KPI Threshold |

| | | | |
|---|---|---|---|
| Other | N/A | N/A | N/A |

# Part B: Performance Monitoring

**Performance Monitoring and Performance Review**

1.1 The Parties shall use good faith efforts to meet within twenty (20) Working Days of the Effective Date in order to mutually agree the details of the process in respect of the monitoring and reporting of Key Performance Indicators and will endeavour to agree such process as soon as reasonably possible, and the Parties agree to align such process with the Quarterly Business Review Meetings for efficiency.

1.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") not to exceed quarterly intervals and in accordance with the process agreed pursuant to Paragraph 1.1 of Part B of this Schedule and with such frequency as shall be agreed between the Parties pursuant to Paragraph 1.1 to enable the Buyer to assess the Supplier's performance against each Key Performance Indicator in each Measurement Period. The Performance Monitoring Reports shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

for each Key Performance Indicator, the actual performance achieved against the KPI Performance Measure for the relevant Service Period and, where a Measurement Period has ended in the period covered by the Performance Monitoring Report, the most recently ended Measurement Period; a summary of all failures to achieve Key Performance Indicators that occurred during that Service Period;

details of any Critical KPI Failures; for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence; the Service Credits to be applied in respect of the relevant period indicating the failures and Key Performance Indicators to which the Service Credits relate; and such other details as the Buyer may reasonably require from time to time in advance in writing.

The Parties shall attend meetings to discuss Performance Monitoring Reports (**"Performance Review Meetings"**) on as part of the Quarterly Business Review Meetings between the Parties. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer and the Supplier mutually agree;

be attended by the Supplier's Representative and the Buyer's Representative; and

The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

The relevant table in the Annex to Part A of this Schedule describes how the levels of performance under the KPI Performance Measures will be mapped to the performance ratings prescribed under regulation 38(5) of the Procurement Regulations 2024. The mapping set out in that table will be applied by the Buyer when publishing relevant Transparency Information relating to the Performance Indicators and/or the Supplier's performance against the relevant KPIs pursuant to Section 52(3) and/or Section 71(2) of the Procurement Act 2023 and the associated Regulations.

The Supplier acknowledges and agrees that, each time the Buyer conducts an assessment of the Supplier's performance against a Key Performance Indicator, the Buyer may publish information as required by Law in relation to that assessment.

**Satisfaction Surveys**

The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

Schedule 2

## AUTHORITY'S MANDATORY TERMS

**A.** For the avoidance of doubt, references to 'the Agreement' mean the attached Call-Off Contract between the Supplier and the Authority. References to 'the Authority' mean 'the Buyer' (the Commissioners for His Majesty's Revenue and Customs).

**B.** The Agreement incorporates the Authority's mandatory terms set out in this Schedule 2.

**C.** In case of any ambiguity or conflict, the Authority's mandatory terms in this Schedule 2 will supersede any other terms in the Agreement.

**D.** For the avoidance of doubt, the relevant definitions for the purposes of the defined terms set out in the Authority's mandatory terms in this Schedule 2 are the definitions set out at Clause 1 of this Schedule 2.

### 1. Definitions

| | |
|---|---|
| **"Affiliate"** | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time; |
| **"Authority Data"** | (a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:<br>(i) supplied to the Supplier by or on behalf of the Authority; and/or<br>(ii) which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or<br>(b) any Personal Data for which the Authority is the Controller, or any data derived from such Personal Data which has had any designatory data identifiers removed so that an individual cannot be identified; |
| **"Charges"** | the charges for the Services as specified in Annex 3; |
| **"Connected Company"** | means, in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person; |
| **"Control"** | the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by |

| | |
|---|---|
| | contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly; |
| **"Controller", "Processor", "Data Subject",** | take the meaning given in the UK GDPR; |
| **"Data Protection Legislation"** | (a) "the data protection legislation" as defined in section 3(9) of the Data Protection Act 2018; and;<br>(b) all applicable Law about the processing of personal data and privacy; |
| **"Key Subcontractor"** | any Subcontractor:<br>(a) which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or<br>(b) with a Subcontract with a contract value which at the time of appointment exceeds (or would exceed if appointed) ten per cent (10%) of the aggregate Charges forecast to be payable under this Call-Off Contract; |
| **"Law"** | any applicable Act of Parliament, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of section 2 of the European Communities Act 1972, regulatory policy, guidance or industry code, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply; |
| **"Personal Data"** | has the meaning given in the UK GDPR; |
| **"Purchase Order Number"** | the Authority's unique number relating to the supply of the Services; |
| **"Services"** | the services to be supplied by the Supplier to the Authority under the Agreement, including the provision of any Goods; |
| **"Subcontract"** | any contract or agreement (or proposed contract or agreement) between the Supplier (or a Subcontractor) and any third party whereby that third party agrees to provide to the Supplier (or the Subcontractor) all or any part of the Services, or facilities or |

| | |
|---|---|
| | services which are material for the provision of the Services, or any part thereof or necessary for the management, direction or control of the Services or any part thereof; |
| **"Subcontractor"** | any third party with whom:<br>(a) the Supplier enters into a Subcontract; or<br>(b) a third party under (a) above enters into a Subcontract, or the servants or agents of that third party; |
| **"Supplier Personnel"** | all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier's obligations under the Agreement; |
| **"Supporting Documentation"** | sufficient information in writing to enable the Authority to reasonably verify the accuracy of any invoice; |
| **"Tax"** | (a) all forms of tax whether direct or indirect;<br>(b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction;<br>(c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions. levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and<br>(d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above,<br>in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction; |
| **"Tax NonCompliance"** | where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC's "Test for Tax Non-Compliance", as set out in Annex 1, where:<br>(a) the "Economic Operator" means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Clause 4.3; and<br>(b) any "Essential Subcontractor" means any Key Subcontractor; |
| **"UK GDPR"** | the UK General Data Protection Regulation, the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679); |

**"VAT"** value added tax as provided for in the Value Added Tax Act 1994.

**2. Payment and Recovery of Sums Due**

2. The Supplier shall invoice the Authority as specified in this Call-Off Contract of the Agreement. Without prejudice to the generality of the invoicing procedure specified in the Agreement, the Supplier shall procure a Purchase Order Number from the Authority prior to the commencement of any Services and the Supplier acknowledges and agrees that should it commence Services without a Purchase Order Number:

   1. the Supplier does so at its own risk; and

   2. the Authority shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.

**2.1** Each invoice and any Supporting Documentation required to be submitted in accordance with the invoicing procedure specified in the Agreement shall be submitted by the Supplier, as directed by the Authority from time to time via the Authority's electronic transaction system.

**2.2** If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Supplier under the Agreement or under any other agreement or contract with the Authority. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.

**3. Warranties**

**3.1** The Supplier represents and warrants that:

**3.1.1** in the three years prior to the Start Date, it has been in full compliance with all applicable securities and Laws related to Tax in the United Kingdom and in the jurisdiction in which it is established;

**3.1.2** it has notified the Authority in writing of any Tax Non-Compliance it is involved in; and

**3.1.3** no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue and the Supplier has notified the Authority of any profit warnings issued in respect of the Supplier in the three years prior to the Start Date.

**3.2** If at any time the Supplier becomes aware that a representation or warranty given by it under Clause

3. 1.1, 3.1.2 and/or 3.1.3 has been breached, is untrue, or is misleading, it shall immediately notify the Authority of the relevant occurrence in sufficient detail to enable the Authority to make an accurate assessment of the situation.

**3.3** In the event that the warranty given by the Supplier pursuant to Clause 3.1.2 is materially untrue, the Authority shall be entitled to terminate the Agreement pursuant to the Call-Off clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

## 4. Promoting Tax Compliance

**4.1** All amounts stated are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Authority following delivery of a valid VAT invoice.

**4.2** To the extent applicable to the Supplier, the Supplier shall at all times comply with all Laws relating to Tax and with the equivalent legal provisions of the country in which the Supplier is established.

**4.3** The Supplier shall provide to the Authority the name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or self-assessment reference of any agent, supplier or Subcontractor of the Supplier prior to the provision of any material Services under the Agreement by that agent, supplier or Subcontractor. Upon a request by the Authority, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Subcontractor supplying Services under the Agreement.

**4.4** If, at any point during the Term, there is Tax Non-Compliance, the Supplier shall:

**4.4.1** notify the Authority in writing of such fact within five (5) Working Days of its occurrence; and

**4.4.2** promptly provide to the Authority:

**(a)** details of the steps which the Supplier is taking to resolve the Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and

**(b)** such other information in relation to the Tax Non-Compliance as the Authority may reasonably require.

**4.5** The Supplier shall indemnify the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under this Agreement. Any amounts due under this Clause 4.5 shall be paid in cleared funds by the Supplier to the Authority not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Authority.

**4.6** Upon the Authority's request, the Supplier shall provide (promptly or within such other period notified by the Authority) information which demonstrates how the Supplier complies with its Tax obligations.

**4.7** If the Supplier:

**4.7.1** fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with Clauses 4.2, 4.4.1 and/or 4.6 this shall be a material breach of the Agreement;

**4.7.2** fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with a reasonable request by the Authority that it must not contract, or must cease to contract, with any agent, supplier or Subcontractor of the Supplier as required by Clause 4.3 on the grounds that the agent, supplier or Subcontractor of the Supplier is involved in Tax Non-Compliance this shall be a material breach of the Agreement; and/or

**4.7.3** fails to provide details of steps being taken and mitigating factors pursuant to Clause 4.4.2 which in the reasonable opinion of the Authority are acceptable this shall be a material breach of the Agreement;

and any such material breach shall allow the Authority to terminate the Agreement pursuant to the Call-Off Clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

**4.8** The Authority may internally share any information which it receives under Clauses 4.3 to 4.4 (inclusive) and 4.6, for the purpose of the collection and management of revenue for which the Authority is responsible.

## 5. Use of Off-shore Tax Structures

**5.1** Subject to the principles of non-discrimination against undertakings based either in member countries of the European Union or in signatory countries of the World Trade Organisation Agreement on Government Procurement, the Supplier shall not, and shall ensure that its Connected Companies, Key Subcontractors (and their respective Connected Companies) shall not, have or put in place (unless otherwise agreed with the Authority) any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description which would otherwise be payable by it or them on or in connection with the payments made by or on behalf of the Authority under or pursuant to this Agreement or (in the case of any Key Subcontractor and its Connected Companies) United Kingdom Tax which would be payable by it or them on or in connection with payments made by or on behalf of the Supplier under or pursuant to the applicable Key Subcontract (**"Prohibited Transactions"**). Prohibited Transactions shall not include transactions made between the Supplier and its Connected Companies or a Key Subcontractor and its Connected Companies on terms which are at arms-length and are entered into in the ordinary course of the transacting parties' business.

**5.2** The Supplier shall notify the Authority in writing (with reasonable supporting detail) of any proposal for the Supplier or any of its Connected Companies, or for a Key Subcontractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall notify the Authority within a reasonable time to allow the Authority to consider the proposed Prohibited Transaction before it is due to be put in place.

**5.3** In the event of a Prohibited Transaction being entered into in breach of Clause 5.1 above, or in the event that circumstances arise which may result in such a breach, the Supplier and/or the Key Subcontractor (as applicable) shall discuss the situation with the Authority and, in order to ensure future compliance with the requirements of Clauses 5.1 and 5.2, the Parties (and the Supplier shall procure that the Key Subcontractor, where applicable) shall agree (at no cost to the Authority) timely and appropriate changes to any such arrangements by the undertakings concerned, resolving the matter (if required) through the escalation process in the Agreement.

**5.4** Failure by the Supplier (or a Key Subcontractor) to comply with the obligations set out in Clauses 5.2 and 5.3 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

## 6 Data Protection and off-shoring

**6.1** The parties agree that the Supplier shall, whether it is the Controller or Processor, in relation to any Personal Data processed in connection with its obligations under the Agreement:

**6.1.1** not process or permit to be processed Personal Data outside of the United Kingdom unless the prior explicit written consent of the Authority has been obtained, an expression of which shall be the incorporation of the processing described in Annex 1 Part A (Data Processing Table) and the following conditions are fulfilled:

**(a)** the Supplier or any applicable Processor has provided appropriate safeguards in relation to any transfer of the Personal Data (whether in accordance with UK GDPR Article 46 or, where relevant, section 75 of the Data Protection Act 2018) as determined by either the Authority or the Supplier when it is the Controller;

**(b)** the Data Subject has enforceable rights and effective legal remedies;

**(c)** the Supplier or any applicable Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is processed (or, if it is not so bound, uses its best endeavours to assist either the Authority or the Supplier when it is the Controller in meeting its obligations); and

**(d)** the Supplier or any applicable Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

**6.2** Failure by the Supplier to comply with the obligations set out in Clause 6.1 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

**6.3** For the sake of clarity, the Authority authorizes, subject to the condition set forth in 6.1 of this section, the Processing of Personal Data outside the United Kingdom by Supplier's Subprocessors in the locations listed in section 14.7.4.3 and Part A, Annex I of the Order Form.

## 7 Commissioners for Revenue and Customs Act 2005 and related Legislation

**7.1** The Supplier shall comply with and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 18 of the Commissioners for Revenue and Customs Act 2005 ('CRCA') to maintain the confidentiality of Authority Data. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the aforesaid obligations may lead to a prosecution under Section 19 of CRCA.

**7.2** The Supplier shall comply with and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 123 of the Social Security Administration Act 1992, which may apply to the fulfilment of some or all of the Services. The Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the Supplier's obligations under Section 123 of the Social Security Administration Act 1992 may lead to a prosecution under that Act.

**7.3** The Supplier shall comply with and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in the Official Secrets Acts 1911 to 1989 and the obligations set out in Section 182 of the Finance Act 1989.

**7.4** The Supplier shall regularly (not less than once every six (6) months) remind all Supplier Personnel who will have access to, or are provided with, Authority Data in writing of the obligations upon Supplier Personnel set out in Clause 7.1 above. The Supplier shall monitor the compliance by Supplier Personnel with such obligations.

**7.5** The Supplier shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data sign (or have previously signed) a Confidentiality Declaration, in the form provided at

Annex 2. The Supplier shall provide a copy of each such signed declaration to the Authority upon demand.

**7.6** In the event that the Supplier or the Supplier Personnel fail to comply with this Clause 7, the Authority reserves the right to terminate the Agreement with immediate effect pursuant to the clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

## 8 Confidentiality, Transparency and Publicity

**8.1** The Supplier shall not, and shall take reasonable steps to ensure that the Supplier Personnel shall not:

8.1.1 make any press announcement or publicise the Agreement or any part of the Agreement in any way; or

8.1.2 use the Authority's name or brand in any promotion or marketing or announcement of orders, except with the prior written consent of the Authority.

**8.2** Each Party acknowledges to the other that nothing in this Agreement either expressly or by implication constitutes an endorsement of any products or services of the other Party and each Party agrees not to conduct itself in such a way as to imply or express any such approval or endorsement.

**8.3** The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the Freedom of Information Act 2000 ("FOIA"), the content of this Agreement is not Confidential Information. The Authority shall be responsible for determining in its absolute discretion whether any of the content of the Agreement is exempt from disclosure in accordance with the provisions of the FOIA. Notwithstanding any other term of this Agreement, the Supplier hereby gives its consent for the Authority to publish the Agreement in its entirety, (*but any information which is exempt from disclosure in accordance with the provisions of the FOIA may be redacted by the Authority*) including from time-to-time agreed changes to the Agreement, to the general public. The Authority may consult with the Supplier to inform its decision regarding any redactions, but the Authority shall have the final decision at its absolute discretion.

**8.4** The Supplier shall assist and cooperate with the Authority to enable the Authority to publish this Agreement.

**Annex 1**

**Excerpt from HMRC's "Test for Tax Non-Compliance"**

*Condition one (An in-scope entity or person)*

1. There is a person or entity ("X") which is either:
   (a) The Economic Operator or Essential Subcontractor ("EOS");
   (b) Part of the same group of companies as EOS. An entity will be treated as within the same group of EOS where that entities' financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts*[1];

[1] https://www.iasplus.com/en/standards/ifrs/ifrs10

(c) Any director, shareholder or other person ("P") which exercises control over EOS. 'Control' means P can secure, through holding of shares or powers under articles of association or other document that EOS's affairs are conducted in accordance with P's wishes.

---

*Condition two (Arrangements involving evasion, abuse or tax avoidance)*

2. X has been engaged in one or more of the following: (a) Fraudulent evasion[2];
   (b) Conduct caught by the General Anti-Abuse Rule[3];
   (c) Conduct caught by the Halifax Abuse principle[2];
   (d) Entered into arrangements caught by a DOTAS or VADR scheme[3];
   (e) Conduct caught by a recognised 'anti-avoidance rule'[4] being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not effected for commercial purposes. 'Targeted Anti-Avoidance Rules' (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;
   (f) Entered into an avoidance scheme identified by HMRC's published Spotlights list[7];
   (g) Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

*Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))*

3. X's activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:
   (a) In respect of 2(a), either X:
      (i) Has accepted the terms of an offer made under a Contractual Disclosure Facility ("CDF") pursuant to the Code of Practice 9 (COP9) procedure[5]; or, (ii) Has been charged with an offence of fraudulent evasion.

---

[2] "Halifax Abuse Principle" means the principle explained in the CJEU Case C-255/02 Halifax and others

[3] A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

[4] The full definition of 'Anti-avoidance rule' can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly.

[7] Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: https://www.gov.uk/government/collections/tax-avoidance-schemes-currently-in-thespotlight

[5] The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed.

[2] 'Fraudulent evasion' means any 'UK tax evasion offence' or 'UK tax evasion facilitation offence' as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act.

[3] "General Anti-Abuse Rule" means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions

(b) In respect of 2(b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB: Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.

(c) In respect of 2(b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.

(d) In respect of 2(f) this condition is satisfied without any further steps being taken.

(e) In respect of 2(g) the foreign equivalent to each of the corresponding steps set out above in 3(a) to (c).

For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time including any implementing or successor legislation.

## Annex 2 Form CONFIDENTIALITY DECLARATION

CONTRACT REFERENCE: SR2497129644 ('the Agreement') DECLARATION:

I solemnly declare that:

1. I am aware that the duty of confidentiality imposed by section 18 of the Commissioners for Revenue and Customs Act 2005 applies to Authority Data (as defined in the Agreement) that has been or will be provided to me in accordance with the Agreement.
2. I understand and acknowledge that under Section 19 of the Commissioners for Revenue and Customs Act 2005 it may be a criminal offence to disclose any Authority Data provided to me.

| |
|---|
| SIGNED: [redacted] |
| FULL NAME: [redacted] |
| POSITION: [redacted] |
| COMPANY: [redacted] |
| DATE OF SIGNATURE: [redacted] |

## Schedule 3- GitLab Subscription Agreement

## (Special Terms 1 to the Contract Between HMRC and GitLab)

### 1. DEFINITIONS

"Acceptance" of an Order Form shall occur at the earliest of the following: (a) execution of an Order Form, (b) reference to an Order Form Quote No. within a purchase order or similar document, or (c) the use of Software.

"Additional Terms" are separate terms and conditions governing Customer's access to and use of certain (a) features in the Software, or (b) Supplemental Services available for purchase, as set forth here: https://about.gitlab.com/terms/.

"Add-On User(s)" are additional Users in excess of those that have been purchased under a Subscription via an executed Order Form or web-portal purchase.

“Affiliate” means any entity(ies) controlling, controlled by, and/or under common control with a party hereto, where “control” means the legal power to direct or cause the direction of the general management of the entity or the ownership of more than 50% of the voting securities in such entity.

“Appendix” are inclusions in these Terms that state the terms by which Software is offered to Customer. The Appendices shall be considered part of the Agreement.

“Authorized Partner” is a reseller or distributor that is enabled and authorized to sell Software.

“Contractors” are defined as third parties that Customer has engaged to manage, or otherwise use the Software, solely on behalf of Customer.

“Controlled Subject Matter” is the Software or any software or anything related thereto or any direct product thereof, collectively.

“Customer Content” is all software, information, content and data provided by or on behalf of Customer or made available or otherwise distributed through the use of the Software.

“Customer Records” collectively means books, records, contracts and accounts relating to the payments due to GitLab under this Agreement.

“Customer Success Services” means adoption services which are provided as part of the Subscription, as set forth in Appendix 1. Customer Success Services include the collection of Operational Data (as further stated in Appendix 1). Customer Success Services are only available to Customers who are purchasing Software, and are not available for Free Software.

“Customer Support” means technical support of the Software provided by GitLab.

“Designated National” is any person or entity on the U.S. Department of Treasury’s List of Specially Designated Nationals or the U.S. Department of Commerce’s Table of Denial Orders.

"Documentation” means the GitLab specific technical specifications, guides and policies; system requirements, and application limits related to GitLab’s Software and Supplemental Services as made available within the Software platform, as set out on the dedicated GitLab Docs Website pages (https://docs.gitlab.com/ee/), or as otherwise referenced on the GitLab Website Pricing Page (https://about.gitlab.com/pricing/). Documentation does not include marketing materials or content published on the Website.

“Effective Price” means the actual price paid by Customer (List Price minus any applicable discount(s)) as set forth on an Order Form or as purchased via the Website.

“Embargoed Countries” refers collectively to countries to which the United States maintains an embargo.

“Enterprise” means the organization, company, corporation and/or other type of entity which procures the Software to be used on its behalf pursuant to the terms of this Agreement.

“Fees” are those fees set forth within the Order Form, or, fees due immediately when purchasing via the web-portal. All Fees are in U.S. Dollars unless otherwise set forth in an Order Form.

“Free Software” means the free, feature-limited version of Software provided to a Customer, User, end user, partner, or any other third party including but not limited to, the lowest tier offering of Software as made available by GitLab and Software provided for evaluation purposes.

“Individual” means a person who uses the Software on their own behalf, and not an Enterprise. An Individual must be over the age of thirteen (13) years old.

“List Price” means the list price of the GitLab Software excluding (if applicable) any discount(s) set forth in an Order Form or as purchased via the Website.

“Order Form” is a transactional document agreed to between the parties which states the Software and/or Supplemental Services being purchased, term of use, price, and other applicable transaction details. For the avoidance of doubt, the parties acknowledge and agree the terms and conditions stated within this Agreement and an executed Order Form shall govern with respect to all matters contemplated herein.

“Purchase Order” is a Customer’s processing document, or similar record, which is used by Customer to demonstrate internal approval and /or record of a purchase. Any terms stated within a Purchase Order shall be null and void and are expressly rejected by the parties.

“Software” means software, and other branded offerings made available by GitLab or its Affiliate(s), including but not limited to, GitLab’s DevOps Lifecycle Application Platform and applicable Supplemental Services and its related Documentation. Software does not include any Testing Features as defined below and as further described in Section 15.3.

“Subscription” refers to the applicable services, support and function(s) of the Software as provided. Subscriptions are provided in tiers / levels as described in Appendix 1 and are based on the number of Users.

“Subscription Start Date” is, unless otherwise agreed to in writing, the start date, (i) stated on an Order Form, or, the date in which Customer is given access to the Software (whichever is later), or (ii) as indicated via a Website transaction, regardless if such purchase is direct with GitLab or via an Authorized Partner.

“Subscription Term” shall begin on the Subscription Start Date and continue for twelve (12) months, unless the term length is otherwise agreed to in an Order Form or web-portal purchase.

“Supplemental Services” means additional capacity, functionality, storage, professional and success services and/or other elements that Customer may procure separately for additional Fees. Supplemental Services may be purchased by Order Form, web-portal, or statement of work as applicable. Supplemental Services will be: (i) provided as a separate line item in an Order Form or web-portal purchase, and (ii) co-termed to the underlying Subscription Term if not purchased on the Subscription Start Date.

"Testing Features” means the experiment, alpha, or beta features that are not ready for production use as further described in Section 15.3.

“User(s)” is defined as the unique and single Individual, employee, Contractor, or other third-party individual or machine authorized by Customer (in accordance with this Agreement) that requires the provision of a seat within the admin platform, who are able to access the Software purchased under a Subscription, regardless of whether the User actually

accesses, or the frequency with which they access, the Software. A User must be over the age of thirteen (13) years old.

“Website” means GitLab’s website located at www.gitlab.com and all subdomains, and all content, services, documentation provided on the Website.

**2. SCOPE OF AGREEMENT; ADDITIONAL TERMS**

2.1 This Agreement establishes a terms that will enable GitLab to provide Customer with the Software. Software is provided as part of a Subscription, as described in Appendix 1. Software provided as a hosted solution, or Software-asa-Service (“SaaS Software”), shall be subject to the attached Appendix 2 entitled “Software as a Service (SaaS) Offering.”

2.3 GitLab Dedicated (Dedicated SaaS) is Software provided as the single-tenant version of GitLab’s SaaS Software, providing Customer dedicated hosting servers and supporting infrastructure, including Primary and Secondary Hosting Location(s), and shall be subject to the attached Appendix 2B entitled “Software as a Service (SaaS) Offering – GitLab Dedicated”.

2.4 Additional Terms will apply to certain features or Supplemental Services that Customer accesses, uses, enables or otherwise purchases, including the provision of artificial intelligence functionality. If there is any conflict between this Agreement and Additional Terms with respect to such features or Supplemental Services, the Additional Terms will control.

**3. ORDERING PROCESS**

3.1 This Agreement applies to Software that Customer licenses directly from GitLab, a GitLab Affiliate, or from an Authorized Partner. For the avoidance of doubt, in the event Customer purchases from an Authorized Partner, GitLab shall have no obligations to Customer with respect to any terms and conditions outside of this Agreement unless otherwise agreed to in writing between Customer and GitLab.

3.2 Unless otherwise agreed to between Customer and GitLab in writing, the terms of this Agreement shall govern any and all use of the Software. Purchases of Software may take place by either:

(i) purchasing via the GitLab Website;

(ii) executing an Order Form with GitLab or an Affiliate of GitLab; or (iii) purchase from an Authorized Partner.

3.3 GitLab and Customer acknowledge and agree that Free Software may be: (i) modified and/or updated, without notice, and (ii) limited in functionality, features, maintenance, support and contain other limitations not present in Software purchased. NOTWITHSTANDING THE “WARRANTY” AND “INDEMNIFICATION” SECTIONS BELOW, FREE SOFTWARE AND SOFTWARE OFFERED ON A TRIAL BASIS (AS STATED IN AN ORDER FORM OR WEB-PORTAL PURCHASE) ARE PROVIDED “AS-IS” WITHOUT ANY WARRANTY AND GITLAB SHALL HAVE NO INDEMNIFICATION OBLIGATIONS NOR LIABILITY OF ANY TYPE WITH RESPECT TO SUCH FREE SOFTWARE UNLESS SUCH EXCLUSION OF LIABILITY IS NOT ENFORCEABLE UNDER APPLICABLE LAW, IN WHICH CASE GITLAB’S LIABILITY WITH RESPECT TO SUCH FREE SOFTWARE SHALL NOT EXCEED $1,000.00USD.

**4. TERM AND TERMINATION; SUSPENSION – Intentionally omitted 5. RESTRICTIONS AND RESPONSIBILITIES**

5.1 Customer will not, and will not permit any third party to (not otherwise defined as a User):

(i) use the Software for any purpose other than as specifically authorized in the Documentation and this Agreement;

(ii) use the Software in violation of the Acceptable Use Policy available at https://about.gitlab.com/terms/#currentterms-of-use;

(iii) use the Software in such a manner that would enable any third party to access the Software;

(iv) use the Software for time sharing or service bureau purposes (including without limitation, sublicensing, distributing, selling, reselling any Software);

(v) for any purpose other than its and its Affiliates' own internal use;

(vi) use the Software other than in compliance with all applicable laws and regulations;

(vii) use the Software in any manner that: (a) is harmful, fraudulent, deceptive, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, or libelous (including without limitation, accessing any computer, computer system, network, software, or data without authorization, breaching the security of another user or system, and/or attempting to circumvent any User authentication or security process); (b) impersonates any person or entity, including without limitation any employee or representative of GitLab; (c) includes content, with respect to the use of SaaS Software, which is illegal or (d) introduces any virus, trojan horse, worm, time bomb, unsolicited bulk, commercial, or "spam" message, or other harmful computer code, file, or program (including without limitation, password guessing programs, decoders, password gatherers, keystroke loggers, cracking tools, packet sniffers, and/or encryption circumvention programs); and

(viii) except to the extent permitted by applicable law, disassemble, reverse engineer, or decompile the Software or access it to: (a) build a competitive product or service, (b) build a product or service using similar ideas, features, functions or graphics of the Software, (c) copy any ideas, features, functions or graphics of the Software, or (d) determine whether the Software are within the scope of any patent.

5.2 Nothing in this Agreement shall prohibit Customer from using the Software for benchmark testing or comparative analysis. Customer will comply with all applicable data privacy and security laws and shall have appropriate technological, administrative, and physical controls in place to ensure such compliance.

5.3 In accordance with this Agreement, GitLab has the right to verify electronically (or otherwise), and generate, or require Customer to generate and provide, reports related to Customer's installation of, access to, and use of the Software to ensure compliance with the terms of this Agreement. GitLab may, upon thirty (30) days' prior written notice to Customer and during Customer's normal business hours and subject to industry-standard confidentiality obligations and Government security requirements, hire an independent third-party auditor to audit the Customer Records only to verify the amounts payable under this Agreement with respect to Customer usage of the Software. If an audit reveals underpayment, Customer shall promptly pay the deficiency to GitLab plus late fees pursuant to Section 6. GitLab shall bear the cost of an audit.

5.4 Customer will be responsible for the following: (i) maintaining the security of Customer's account, passwords (including, but not limited to, administrative and User passwords) and files, and for all uses of Customer account

with or without Customer's knowledge or consent; and (ii) any acts or omissions carried out by Contractors on Customer's behalf. Customer shall ensure that Contractors are subject to terms no less stringent than those stated herein.

5.5 Subject to this Agreement and the applicable Order Form, GitLab will provide Customer Support to Customer for the Subscriptions, during the Subscription Term, at no additional cost. Details regarding Customer Support can be found in Appendix 1, as well as at https://about.gitlab.com/support, as updated from time to time.

5.6 Portions of the Software are governed by underlying open source licenses as described at https://docs.gitlab.com/ee/development/licensing.html. This Agreement and applicable Appendix(eces) establish the rights and obligations associated with Subscriptions and Software and are not intended to limit Customer's right to software code under the terms of an open source license.

5.7 Customer acknowledges and agrees that:

(i) Account names are administered by GitLab on a "first come, first serve" basis;

(ii) Intentional name squatting, or purchasing, soliciting, or selling of an account name is prohibited; and (iii) GitLab reserves the right to remove, rename, or close inactive accounts at its discretion.

**6. PAYMENT OF FEES**

6.1 With respect to purchases direct from GitLab, all web-portal purchase Fees shall be due and payable immediately.

6.2 With respect to purchases direct from GitLab, the Order Form shall: (i) reference this Agreement; (ii) state the Subscription Term(s) and Subscription(s) that are being purchased; and (iii) state the Fees due for the applicable Subscription(s).

6.3 With respect to purchases direct from GitLab, such Order Form is hereby incorporated into this Agreement by reference. The parties hereby agree to the terms and conditions stated within this Agreement and those found within an Order Form to the exclusion of all other terms. The parties agree that all terms stated within a Purchase Order, or other similar document, shall be null and void and are expressly rejected.

6.4 With respect to purchases direct from GitLab, Customer will pay GitLab the applicable Fees, without any right of setoff or deduction. All payments will be made in accordance with the payment details stated within the applicable Order Form. If not otherwise specified: (i) GitLab (or applicable GitLab Affiliate) will invoice Customer for the Fees upon the Acceptance of an Order Form; and (ii) all undisputed Fees will be due and payable within thirty (30) days of Customer's receipt of an invoice. Except as expressly set forth in this Agreement, all Fees paid or due hereunder (including prepaid amounts) are non-refundable, and no credit will be due, including without limitation if this Agreement is terminated in accordance with Section 4 herein. For the avoidance of doubt, Fees shall be in U.S. Dollars unless otherwise set forth in an Order Form.

6.5 During the Subscription Term, Customer may, subject to this Agreement, activate and use Add-On Users. For the avoidance of doubt, Customer shall not have the right to report less than the number of Users originally purchased under the Subscription, and all Add-On Users shall be co-termed to the underlying Subscription Term.

6.6 With respect to purchases direct from GitLab, at the end of each three (3) month period, commencing up on the Subscription Start Date, (referred to herein as "Quarter" or "Quarterly") during the Subscription Term, GitLab will: (i) per

Section 5.3, generate a report of Add-On User(s) activated and/or used during the Quarter ("Quarterly Usage Report"), and (ii) invoice Customer on a prorated basis for the remaining portion of the Subscription Term, with respect to the Add-On User(s) activated and/or used during the Quarter as captured by the Quarterly Usage Report. For the avoidance of doubt, Add-On User(s) will not be invoiced for the Quarter in which they were activated and/or used. A Quarterly Usage Report will be generated during the first three (3) Quarters of a Subscription Term. Upon expiration of the Subscription Term, Customer's renewal of the Software shall be for the same number of User licenses purchased for the most recent Subscription Term, plus any Add-On Users activated and/or used during such Subscription Term, unless otherwise agreed to between the parties. Add-On User(s) that have been identified within the Quarterly Usage Report, shall be considered due and payable in accordance with this Section 6. In the event a Quarterly Usage Report cannot be generated, Customer shall report and pay for such Overage Users (as defined below) in compliance with Section

6.7. Unless the parties agree to an Effective Price for Add-On Users which is less than the List Price, as set forth in an Order Form or Website purchase, Add-On Users activated and/or used during a Subscription Term will be invoiced at the List Price in the most recent Order Form or Website purchase.

6.7 In the event a Customer procures Software from an Authorized Partner, or, GitLab is unable to: (i) verify and generate a Quarterly Usage Report, and/or (ii) collect payment(s) with respect to Quarterly Add-Ons as provided in the Quarterly Usage Report, Customer shall be obligated to: (a) provide a report no later than twelve (12) months following the Subscription Effective Date ("Annual Report") of all Users from said Subscription Term ("Overage Users"), and (b) be obligated to pay for such Overage Users, for the previous twelve (12) months, at the then current List Price for the GitLab Software. Overage Users subject to the Annual Report shall not include any pro-ration, set-off and/or deduction to account for term of use, or otherwise. Overage Users that have been identified in an Annual Report shall be considered due and payable in accordance with Section 6. In the event Overage Users are outstanding upon the expiration of a Subscription Term, Customer shall be obligated to pay for such Overage Users in order to renew the Software.

6.8 Any unpaid Fees are subject to a finance charge of one percent (1.0%) per month, or the maximum permitted by law, whichever is lower, plus all expenses of collection, including reasonable attorneys' fees. Fees under this Agreement are exclusive of any and all taxes or duties, now or hereafter imposed by any governmental authority, including, but not limited to any national, state or provincial tax, sales tax, value-added tax, property and similar taxes, if any. Fees under this Agreement shall be paid without any withholding or deduction. In the case of any deduction or withholding requirements, Customer will pay any required withholding itself and will not reduce the amount to be paid to GitLab on account thereof.

**7. CONFIDENTIALITY – Intentionally omitted.**

**8. INTELLECTUAL PROPERTY RIGHTS**

8.1 Subject to the terms and conditions of this Agreement, GitLab hereby grants to Customer and its Affiliates:

(i) with respect to SaaS Software, a limited, non-exclusive, non-transferable, non-sublicensable right to access and use the SaaS Software;

(ii) with respect to Software downloaded and deployed on the Customer's infrastructure (i.e. self-managed), a limited, non-exclusive, non-transferable, non-sublicensable license to download, deploy, and use the Software.

In each case , unless otherwise set forth in an Order Form, Customer's use rights will be limited (a) to the tier level selected via web direct or Order Form purchase where such selected tier (e.g. Premium/Ultimate) may not be commingled with another tier; (b) exclusively for internal use in connection with the development of Customer's and/or its Affiliates' own software; and (c) to the number of Users for which Customer has paid GitLab. Notwithstanding anything to the contrary, Customer agrees that GitLab and/or its licensors (as applicable) retain all right, title and interest in and to all Software, and all Software may only be used in full compliance with this Agreement and with a valid Subscription for the correct number of Users.

8.2 Except as expressly set forth herein, GitLab (and its licensors, where applicable) will retain all intellectual property rights relating to the Software and any suggestions, ideas, enhancement requests, feedback, or other recommendations provided by Customer, its Affiliates, Users or any third party relating to the Software (herein referred to as "Feedback Materials"), which are hereby assigned to GitLab. For the avoidance of doubt, Feedback Materials shall not include Customer Confidential Information or intellectual property owned by Customer. This Agreement does not constitute a sale of the Software and does not convey to Customer any rights of ownership in or related to the Software or any other intellectual property rights.

8.3 Customer shall not remove, alter or obscure any of GitLab's (or its licensors') copyright notices, proprietary legends, trademark or service mark attributions, patent markings or other indicia of GitLab's (or its licensors') ownership or contribution from the Software.

8.4 Subject to Section 8.5, Customer represents it shall be responsible for, and retain all right, title, and interest in and to, Customer Content, subject to a limited license to GitLab necessary for GitLab's provision of the Software and its development and improvement.

8.5 If Customer applies a license to publicly-available Customer Content within the Software, Customer (i) licenses that Customer Content under the terms of the applicable license; and (ii) represents that Customer has sufficient rights in that Customer Content to do so.

**9. WARRANTY**

9.1 During the Subscription Term, GitLab represents and warrants that: (i) it has the authority to enter into this Agreement; (ii) the Software shall be provided in a professional and workmanlike manner by qualified personnel; and (iii) it will use commercial industry standard methods designed to ensure the Software provided to Customer does not include any computer code or other instructions, devices or techniques, including without limitation those known as disabling devices, trojans, or time bombs, that are intentionally designed to disrupt, disable, harm, infect, defraud, damage, or otherwise impede in any manner, the operation of a network, computer program or computer system or any component thereof, including its security or User data.

9.2 If at any time GitLab fails to comply with the warranties in this Section 9, Customer may promptly notify GitLab in writing of any such noncompliance. GitLab will, within thirty (30) days of receipt of such written notification, either correct the noncompliance or provide Customer with a plan for correcting the noncompliance. If the noncompliance is not corrected or if a reasonably acceptable plan for correcting the non-compliance is not established during such period, Customer may terminate this Agreement and receive a prorated refund for the unused portion of the Subscription Term as its sole and exclusive remedy for such noncompliance.

9.3 EXCEPT AS SPECIFICALLY SET FORTH IN THIS AGREEMENT, THE SOFTWARE, SUPPLEMENTAL SERVICES AND CONFIDENTIAL INFORMATION AND ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT ARE PROVIDED "AS-IS," WITHOUT ANY WARRANTIES OF ANY KIND. GITLAB AND ITS LICENSORS HEREBY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT.

**10. INDEMNIFICATION**

10.1 GitLab will defend Customer from any claim, demand, suit or proceeding made or brought against Customer by a third party alleging the Software (excluding Free Software as set forth in Section 3.3) provided by GitLab infringes or misappropriates such third party's patent, copyright, trademarks, or trade secrets (a "Customer Claim"). GitLab will indemnify and hold Customer harmless from any damages, reasonable attorneys' fees and costs finally awarded against Customer as a result of a Customer Claim, or for amounts paid by Customer under a settlement approved (in writing) by GitLab, provided Customer: (i) promptly notifies GitLab in writing of the Customer Claim; (ii) gives GitLab all reasonable assistance at GitLab's expense; and (iii) gives GitLab sole control over defense and settlement thereof except that GitLab may not settle any Customer Claim unless it unconditionally releases Customer of all liability. The foregoing obligations do not apply if: (v) the Customer Claim arises from Software, or any part thereof, that is modified by Customer, or at Customer's direction, after delivery by GitLab; (w) the Customer Claim arises from the use or combination of the Software or any part thereof with other products, processes or materials not provided by GitLab where the alleged infringement relates to such combination; (x) Customer continues allegedly infringing activity after being notified thereof or after being informed of modifications that would have avoided the alleged infringement; (y) the Customer Claim arises from software not created by GitLab, or (z) the Customer Claim results from Customer's breach of this Agreement and/or applicable Order Forms. Notwithstanding the foregoing, in the event of a Customer Claim, GitLab, at its discretion, option and expense, reserves the rights to: (a) modify the Software to make it non-infringing provided there is no material loss of functionality; (b) settle such claim by procuring the right for Customer to continue using the Software; or (c) if in GitLab's reasonable opinion neither (a) or (b) are commercially feasible, terminate the license to the Software and refund a pro-rata portion of the amount paid by Customer for such Software for the unused portion of the Subscription Term.

10.2 Customer will defend GitLab and its Affiliates against any claim, demand, suit or proceeding made or brought against GitLab by a third party alleging: (i) that any Customer Content or Customer's use of Customer Content with the Software or any software (or combination of software) provided by Customer and used with the Software, infringes or misappropriates such third party's intellectual property rights, or (ii) that Customer uses the Software in an unlawful manner or in violation of the Agreement, the applicable Documentation, or Order Form (each a "GitLab Claim"). Customer will indemnify GitLab from any damages, reasonable attorneys' fees and costs finally awarded against GitLab as a result of, or for any amounts paid by GitLab under a settlement approved (in writing) by Customer of a GitLab Claim, provided GitLab: (x) promptly gives Customer written notice of the GitLab Claim, (y) gives Customer sole control of the defense and settlement of the GitLab Claim (except that Customer may not settle any GitLab Claim unless it unconditionally releases GitLab of all liability), and (z) gives Customer all reasonable assistance, at Customer's expense. The above defense and indemnification obligations do not apply if a GitLab Claim arises from GitLab's breach of this Agreement and/or applicable Order Form.

10.3 This Section 10 (Indemnification) states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against the other party for any third-party claim described in this section.

**11. LIMITATION OF LIABILITY – intentionally omitted 12. U.S. GOVERNMENT MATTERS**

12.1 Notwithstanding anything else, Customer acknowledges that Controlled Subject Matter is subject to trade control laws and regulations, including the U.S. Export Administration Regulations ("EAR") and various sanctions programs administered by the U.S. Office of Foreign Assets Control ("OFAC"). Customer shall not export, re-export, or transfer the Controlled Subject Matter except as authorized by these laws and regulations.

12.2 Without limiting the foregoing, Customer shall not export, re-export, or transfer the Controlled Subject Matter without authorization (i) to any Embargoed Country or region, including Cuba, Iran, North Korea, Syria, or the Crimea, Donetsk, and Luhansk regions of Ukraine, (ii) to Russia or Belarus; (iii) to any party identified on or subject to the limitations of OFAC's Specially Designated Nationals List, the Bureau of Industry and Security's Entity, Unverified, or Denied Persons Lists, or (iv) for any end use or end user prohibited by 15 C.F.R. 744, including, without limitation, proliferation activities relating to nuclear, missile, or chemical and biological weapons.

12.3 Use of the Software is representation and warranty that the Customer, Customer personnel, or Contractors are not located in, under the control of, or a national or resident of an Embargoed Country or a Designated National.

12.4 As defined in FAR section 2.101, any software and documentation provided by GitLab are "commercial items" and according to DFAR section 252.2277014(a)(1) and (5) are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with DFAR section 227.7202 and FAR section 12.212, any use modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

**13. FORCE MAJEURE – Intentionally omitted.**

**14. SECURITY / DATA PROTECTION**

14.1 Without limiting GitLab's obligations as stated in Section 7 (Confidentiality), GitLab shall be responsible for establishing and maintaining a commercially reasonable information security program that is designed to: (i) ensure the security and confidentiality of the Customer Content; (ii) protect against any anticipated threats or hazards to the security or integrity of the Customer Content; (iii) protect against unauthorized access to, or use of, the Customer Content; and (iv) ensure that all subcontractors of GitLab, if any, comply with all of the foregoing. In no case shall the safeguards of GitLab's information security program be less stringent than the information security safeguards used by GitLab to protect its own commercially sensitive data. Customer shall use commercially reasonable security and anti-virus measures when accessing and using the Software and to prevent unauthorized access to, or use of the Software, and notify GitLab promptly of any such unauthorized access or use of which it becomes aware.

14.2 With respect to the protection of information, the GitLab Privacy Statement located here https://about.gitlab.com/privacy/, shall apply. If this Agreement is entered into on behalf of an Enterprise, the data processing terms set out in the Contract shall apply to the extent Customer Content includes Personal Data. To the extent Personal Data from the European Economic Area (EEA), the United Kingdom and Switzerland are processed by GitLab, the EU SCCs (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) and the UK ITDA

(https://ico.org.uk/media2/migrated/4019538/international-data-transfer-agreement.pdf) shall apply, as further set forth in Section 14.7.4.3 of the Conditions. For the purposes of the EU SCCs and UK ITDA, Customer and its applicable Affiliates are each the data exporter, and Customer's acceptance of this Agreement, and an applicable Affiliate's execution of an Order Form, shall be treated as its execution of the EU SCCs and UK ITDA.

14.3 The parties acknowledge and agree that: (i) the Software is not designed for the purpose(s) of storing, processing, compiling or transmitting Sensitive Data (as defined herein), and (ii) Customer shall not use the Software, or otherwise provide to GitLab without prior written consent, Sensitive Data under this Agreement. “Sensitive Data” means: (a) special categories of data enumerated in European Union Regulation 2016/679, Article 9(1) or any successor legislation; (b) patient, medical, or other protected health information regulated by the Health Insurance Portability and Accountability Act (as amended and supplemented) (“HIPAA”); (c) credit, debit, or other payment card data or financial account information, including bank account numbers or other personally identifiable financial information; (d) social security numbers, driver’s license numbers, or other government identification numbers; (e) other information subject to regulation or protection under specific laws such as the Children’s Online Privacy Protection Act or Gramm-Leach-Bliley Act (“GLBA”) (or related rules or regulations); or (f) any data similar to the above protected under foreign or domestic laws. Customer further acknowledges that the Software and related features are not intended to meet any legal obligations for these uses, including HIPAA and GLBA requirements, and that GitLab is not a Business Associate as defined under HIPAA. Therefore, notwithstanding anything else in this Agreement, GitLab has no liability for Sensitive Data processed in connection with Customer’s use of the Software.

14.4 To the extent Customer has Users of the SaaS Software located in the People’s Republic of China, or transfers Personal Data to a Dedicated instance from the People’s Republic of China, Customer represents and warrants that it has complied with all requirements of a “personal information processor,” as that term is defined under the Personal Information and Protection Law of the People’s Republic of China (“PIPL”). This includes the requirement to provide adequate notice and obtain all necessary consents from relevant Users prior to the overseas transfer and processing of Personal Data by GitLab, as well as onward transfers and processing by GitLab’s third-party subprocessors. In addition, Customer warrants, where required, that it will not transfer Personal Data without a security assessment, as described in PIPL, from the Cyberspace Administration of China. Nothing in this section limits GitLab or Customer’s obligations under the DPA.

**15. MISCELLANEOUS**

15.1 GitLab may, from time to time, offer certain experimental or beta features or products in the Software and Customer acknowledges and agrees that (i) access to and use of Testing Features will be governed by the Testing Agreement available at: https://about.gitlab.com/terms/ and (ii) Customer’s access or use of such Testing Features will constitute Customer’s acceptance of such Testing Agreement.

15.2 In addition to any rights that accrued prior to termination, the provisions of Sections 3.3, and 5 through 15 shall survive any termination of this Agreement.

**APPENDIX 1: GitLab Subscriptions**

Fees for the Subscriptions are based upon the number of Users and the applicable level of support and/or functionality of the Software, as set forth in the table below. In the event Customer does not reasonably comply with written specifications or instructions from GitLab's service engineers, regarding any support issue or request (including without limitation, failure to make backups of Customer Content or versions of Software) (each, a "Support Issue"), GitLab may cease its support obligations to Customer with respect to such Support Issue upon fifteen (15) days written notice and Customer's inability to cure such noncompliance within the notice period.

**SUBSCRIPTIONS AND LEVELS OF SUPPORT**

| **Subscription*** | **Level of Support (*First Response Time*)** | **Support Details** |
|---|---|---|
| Free *(Formerly "Core" or "Free")* | GitLab Community Forum | |
| Starter *(F.K.A "Basic" or "Bronze")* | GitLab Standard Support | 24 x 5 Support Next business day response (24 hour SLA) Submit Tickets at https://support.gitlab.com |
| Premium *(Formerly Premium or Silver)* | Priority Support (Based upon Support Impact **) | See Priority Support Overview https://support.gitlab.com |
| Ultimate *(Formerly Gold or Ultimate)* | Priority Support (Based upon Support Impact**) | See Priority Support Overview https://support.gitlab.com |

*Note: Subscription names are subject to change, however, the applicable Subscription for that tier shall remain the same during a Subscription Term.

**Support Impact categories are defined at: https://about.gitlab.com/support/#definitions-of-support-impact **PRIORITY**

**SUPPORT OVERVIEW:** https://about.gitlab.com/support/#priority-support

**CUSTOMER SUCCESS SERVICES**

Customer Success Services include additional assistance with respect to Customer's use of the GitLab Software. Customer Success Services are provided at no charge, an overview of the Customer Success Services can be found at https://about.gitlab.com/services/customer-success-services/. In order to receive Customer Success Service(s), Customer acknowledges and agrees that additional data and information ("Operational Data") will be collected. An overview of Operational Data can be found at: https://gitlab-org.gitlab.io/growth/product-intelligence/metricdictionary/?data_category=operational.

## APPENDIX 2: Software as a Service (SaaS) Offering

With respect to Customer's purchase and/or use of the SaaS Software, the following additional terms shall apply.

### AVAILABILITY

Availability to the SaaS Software will be measured, and reported on, by GitLab using instrumentation and observation tools specifically designed to provide a representative measure of service availability. Recent status, references to availability measurement definition, and historical reporting will be available at or linked from the GitLab system status site located at https://about.gitlab.com/handbook/engineering/monitoring/#gitlabcom-service-level-availability.

### RESILIENCY

GitLab will architect and maintain an underlying cloud infrastructure with commercially reasonable resiliency for all data, compute, and network services. At a minimum, GitLab will maintain the highest documented level of "GitLab Reference Architecture" as detailed at https://docs.gitlab.com.

### BACKUPS

GitLab will maintain a commercially reasonable system of data backup process and technology to ensure that primary data sources remain recoverable in the event of various system failures.

### MONITORING AND INCIDENT RESPONSE

GitLab will employ a system of instrumentation and observation tools to ensure that system behavior which may limit use of the SaaS Software is detected and announced. GitLab will also employ industry reasonable practices to maintain appropriate engineering personnel availability for the purposes of incident response(s).

### UPDATES AND UPGRADES

GitLab will update the SaaS Software as updates are available and when reasonably practical to implement said updates. Update timing and process will remain at GitLab's discretion.

### SCHEDULED SYSTEM MAINTENANCE

GitLab will occasionally perform scheduled system maintenance which requires limits to the use of part or all of the SaaS Software features, or significantly reduces features and functions during the scheduled system maintenance period. GitLab will provide ten (10) business days' notice for all scheduled system maintenance activities. GitLab will take a proactive approach to minimizing the need for such maintenance and will limit scheduled system maintenance to less than four (4) hours per calendar month. Notwithstanding the foregoing, in the event of an emergency or urgent issue which may negatively impact GitLab's customers, GitLab has the right to carry out unscheduled maintenance to remedy such instance(s). For the avoidance of doubt, such unscheduled maintenance shall: (i) be limited to only those issues which may negatively impact customers; and (ii) will be carried out in such a manner to provide for the least amount of disruption to customers.

### SUSPENSION OF SERVICE

GitLab reserves the right to suspend service to the SaaS Software in the event of a Suspension Event pursuant to

Section 4.4 of the Agreement including (i) Customer's failure to comply with the Agreement and this Appendix; (ii) Customer exceeding the set application limits published within the Documentation; or (iii) requests or usage deemed malicious in nature and identified to be sourced from Customer accounts, personnel, or systems.

**APPENDIX 2B: Software as a Service (SaaS) Offering - Dedicated SaaS**

With respect to Customer's purchase and/or use of Dedicated SaaS (defined below), the following additional terms shall apply. This Dedicated SaaS offering shall be governed by the terms of the Agreement between the parties and this Appendix 2B. Capitalized terms not defined in this Appendix 2B shall have the meanings ascribed to them in the Agreement.

**1. DEFINITIONS**

"**Hosting Location**" means the physical operation(s) provided to host Dedicated SaaS (as defined herein). This includes all hardware utilized in the provision of services located behind the Service Demarcation Point. Hosting Location includes the Primary Hosting Location and Secondary Hosting Locations(s) (defined below), as applicable.

"**Disaster**" means any catastrophic failure, including but not limited to, flood, earthquake, power loss, internet connectivity loss, major hardware failure, or malicious attack, outside of GitLab's reasonable control, that renders the Primary and/or Secondary Hosting Location(s) inoperable and without an imminent indication of recovery.

"**Dedicated SaaS**" means the single-tenant version of GitLab's SaaS Software, providing Customer dedicated hosting servers and supporting infrastructure, including Primary and Secondary Hosting Location(s).

"**Downtime**" means the material unavailability of Dedicated SaaS preventing Users from accessing and using all aspects and features of Customer's Dedicated SaaS Subscription. Downtime does not include (1) Scheduled System Maintenance or (2) unavailability due to Emergency Events.

"**Downtime Credit"** is a prorated amount of the Fees attributable to Downtime that causes the Service Level Availability of Dedicated SaaS to not meet or exceed the Service Level Objective ("SLO") as defined herein.

"**Emergency Event**" means the occurrence of certain events outside of GitLab's reasonable control that may impact the availability or security of Dedicated SaaS features, including: (i) a Disaster, (ii) Customer's misuse or misconfiguration of Dedicated SaaS, or (iii) other critical, urgent, or severe issues caused by Customer or another third-party, including but not limited to critical security vulnerabilities or data consistency issues. Customer acknowledges and agrees that an Emergency Event may require Unscheduled System Maintenance.

"**End-to-end**" is defined as from the User's desktop to GitLab's hosted routers.

"**Incident**" is defined as a material failure of hardware or Services and Features (as defined in Section 3) or an event that results in significant performance degradation or system unavailability.

"**Service Level Availability**" means the sum of qualifying service level indicators of the Services and Features (as defined in Section 3) in a month, divided by the sum of total qualifying requests of the Services and Features in a month. Further information regarding Service Level Availability is available at https://about.gitlab.com/handbook/engineering/infrastructure/team/gitlabdedicated/slas/#availability-score-calculation. Service Level Availability does not include Downtime resulting from (1) misuse or misconfiguration of Dedicated SaaS, (2) components or services provided with Dedicated SaaS, (3) factors outside of GitLab's reasonable control, such as Disasters or Force Majeure Events, or (4) Customer's or selected cloud hosting providers services, equipment or other technologies. Scheduled System Maintenance or Unscheduled System Maintenance necessary to address critical issues (e.g., security vulnerabilities, data consistency issues, etc.) are also not included in the calculation of Service Level Availability.

"**Scheduled System Maintenance**" means GitLab's weekly maintenance activities related to Customer's Dedicated SaaS Subscription including, but not limited to, instance upgrades, configuration changes, and planned weekly failovers to the Secondary Hosting Location for End-to-end validation of applicable disaster recovery plans.

"**Unscheduled System Maintenance**" means any other maintenance activities outside of Scheduled System Maintenance that GitLab may engage in to prevent, alleviate, or otherwise minimize: (1) Downtime, (2) Emergency Events, or (3) remediating critical security vulnerabilities that do not cause Downtime or Emergency Events.

"**Service Demarcation Point**" means GitLab's border router that is used to establish connectivity from the hosting facility to the public Internet. GitLab is responsible for delivery of Dedicated SaaS access capabilities to and including the Service Demarcation Point.

"**System Availability**" means the availability of Dedicated SaaS for general use by Customer and represents the combined availability of networks, servers, and Dedicated SaaS.

"**System Availability Period**" means, except as otherwise provided herein, 24 hours per day, seven days per week, except for agreed System Maintenance Periods.

"**System Maintenance Period**" means the time period(s) during which Dedicated SaaS access may not be available because of Scheduled System Maintenance or Unscheduled System Maintenance.

**2. RESTRICTIONS AND RESPONSIBILITIES**

Customer is purchasing Subscriptions to Dedicated SaaS. GitLab will provide certain services and features with Customer's purchase of a Dedicated SaaS Subscription as more fully described in Section 5, below. Furthermore, GitLab will be responsible for maintaining ISP network connectivity capable of servicing the relevant internet traffic to and from Dedicated SaaS.

Customer may connect to Dedicated SaaS using the internet, or a private network connection. If Customer elects to connect to Dedicated SaaS through the internet, Customer is responsible for providing its own ISP connection. If Customer elects to connect to Dedicated SaaS using a private network connection, Customer is responsible for managing any required network connections to the Primary and Secondary Hosting Location(s) (defined below). Customer shall also be responsible for ensuring that its configuration is valid and available bandwidth meets the minimum product specifications for Customer's desired level of performance.

During Customer's onboarding to the Dedicated SaaS platform, Customer may choose its primary and secondary Hosting Locations for its Dedicated SaaS servers (respectively, the "Primary Hosting Location" and "Secondary Hosting Location") from a list of approved Primary and Secondary Hosting Locations provided by GitLab. Primary and Secondary Hosting Location(s) may not be changed unless authorized by GitLab in writing. In addition, GitLab shall have the right to modify the underlying infrastructure for which the Dedicated SaaS is installed provided that, (i) such modification shall not materially reduce Customer's use of the Dedicated SaaS, and (ii) does not modify the Primary and/or Secondary Hosting Location (s).

Customer acknowledges and agrees that the following license restrictions shall apply to its Dedicated SaaS Subscription(s), in addition to those identified in the Agreement, including but not limited to Section 5 (*Restrictions and Responsibilities*) thereto: (i) Customer's Subscription to Dedicated SaaS shall be hosted on infrastructure selected and managed by GitLab only; (ii) Customer's Subscription to Dedicated SaaS will not be provided for installation on Customer's infrastructure (whether virtual or physical); and (iii) in the event of termination or expiration of the Agreement, Customer shall be solely responsible for migrating any and all Customer Content and Customer Confidential Information off of GitLab's selected infrastructure to a location of Customer's choosing.

**3. SERVICE LEVEL AVAILABILITY AND SERVICE LEVEL OBJECTIVE**

During the Subscription Term, the Service Level Availability of Dedicated SaaS will be at least 99.5% (the "**Service Level Objective**" or "**SLO**"). Recent status, references to availability measurement definition, and historical reporting will be available to Customer upon request. GitLab will calculate the Service Level Availability based on the availability of certain site services and corresponding features provided with Dedicated SaaS ("Services and Features"). The Service Level Availability calculation and a summary of the Site Services and Features are available at https://about.gitlab.com/handbook/engineering/infrastructure/team/gitlabdedicated/slas/, as updated from time to time. If the

Service Level Availability does not meet or exceed the SLO based on the Service Level Availability calculation, Customer may be entitled to Downtime Credits as set forth in Section 4.

**4. DOWNTIME CREDITS**

On a month-by-month basis, if Service Level Availability does not meet or exceed the SLO stated Section 3 due to Downtime, and provided that Customer has met its obligations under this Appendix 2B and the Agreement, GitLab will credit Customer with a Downtime Credit. In no event shall the Downtime Credit be greater than ten percent (10%) of the Fees paid by Customer for that month.

In order to receive the Downtime Credit, Customer must notify GitLab within ten (10) days from the time Customer becomes eligible to receive the Downtime Credit. If Customer does not comply with this requirement, Customer forfeits its right to receive a Downtime Credit.

If a dispute arises with respect to the Downtime, GitLab will make a determination in good faith based on its system logs, monitoring reports, and any other available information which GitLab will make available to Customer for auditing, upon Customer's request.

Downtime Credit will be applied towards the next payment of Fees due from Customer. This remedy shall be Customer's sole and exclusive remedy for any failure by GitLab to meet the SLO, and is in lieu of all other remedies.

**5. SERVICES DESCRIPTION**

This Section 5 describes the operating characteristics and environment of Dedicated SaaS.

**5.1 SYSTEM MAINTENANCE PERIODS**

GitLab will strive to maximize System Availability, subject to the following System Maintenance Periods:

A. Scheduled System Maintenance. GitLab will perform weekly Scheduled System Maintenance at a date and time as reasonably agreed by the parties. GitLab will proactively limit the Scheduled System Maintenance to no more than four (4) hours per week. Customer acknowledges and agrees that Scheduled System Maintenance may require limits to use of part or all of the Dedicated SaaS features, or significantly reduces features and functions of Dedicated SaaS.

B. Unscheduled System Maintenance. GitLab will provide notice to Customer, as soon as commercially practicable, of any Unscheduled System Maintenance. For the avoidance of doubt, such Unscheduled System Maintenance shall: (i) be limited to only those issues which are time-sensitive for the availability or security of Dedicated SaaS, such as Downtime or Emergency Events, and (ii) will be carried out in such a manner to provide the least amount of disruption to Customer. Customer acknowledges and agrees that GitLab may also engage in Unscheduled System Maintenance, from time to time, in an attempt to prevent, alleviate, or otherwise minimize an Emergency Event, such as a critical security vulnerability. Customer acknowledges and agrees that Unscheduled System Maintenance may require limits to use of part or all of the Dedicated SaaS features, or may significantly reduce features or functions of Dedicated SaaS.

**5.2 Dedicated SaaS Services**

GitLab, through infrastructure selected and managed by GitLab, will provide certain services for a Dedicated SaaS Subscription to ensure Customer's access and use of Dedicated SaaS on the applicable website ("**Site**") in accordance with the provisions below. Such services for Dedicated SaaS will include:

Security – GitLab will use various security measures designed to restrict and monitor access to GitLab systems and Customer Content. Further, GitLab will utilize security controls and tooling designed to protect Customer Content and prevent the unauthorized access and compromise of GitLab servers and endpoints. GitLab will equip and configure the hosting network with controls designed to prevent unauthorized network access from other subnets within the GitLab platform. GitLab will employ security controls to detect network attacks and take appropriate measures should an incident occur. GitLab will have vulnerability scans performed on the Site to detect vulnerabilities and provide recommendations for corrective actions. All application servers will have technical security controls in place designed to prevent the introduction of malicious software and support the detection and eradication of malicious software.

Facilities – Dedicated SaaS includes Primary and Secondary Hosting Locations(s) to support Customer's remote access to the GitLab platform. Dedicated SaaS is deployed on an Infrastructure as a Service (IaaS) and GitLab inherits physical and environmental controls from the service IaaS provider. The Primary and Secondary Hosting Location(s) will restrict physical access to authorized parties only and employ the use of cameras, security guards, and locked cabinets. Hosting Locations will use regulated and redundant power supplies, environmental regulation systems (e.g., moisture detection, temperature regulation), fire detection and suppression equipment, HVAC systems and continual system monitoring to ensure System Availability.

Availability - GitLab will, on a continual basis, monitor the Site and will use its reasonable efforts to keep the Site fully and completely accessible to Customer during the System Availability Period, unless there is an event beyond the reasonable control of GitLab (or an infrastructure provider) that interrupts Site accessibility. System Availability will be measured and reviewed each month. There may be scheduled System Maintenance Periods during which access to the Site may be unavailable. GitLab will make availability data available to customers as detailed in Section 3.

Disaster - In the event of a Disaster, GitLab will restore the Dedicated SaaS service as quickly as possible and will provide notice, to the extent possible, as to the estimated recovery time of the Hosting Location(s).

Redundancy - The network will support high availability and fault tolerance through the use of multiple web, application and database servers, and redundant networking devices, including routers, firewalls, switches and load balancing devices and will support public Internet access through diverse paths.

Monitoring – GitLab employs system monitoring software for the purpose of monitoring and measuring System Availability.

Security Scans - GitLab will contract with a third party to perform regular security audits including all scoped systems and services. Any identified vulnerabilities will be resolved with security patches or configuration changes at the earliest possible time.

Emergency Events - In the event of an Emergency Event preventing Customer's access to and use of Dedicated SaaS, GitLab will restore access and use of Dedicated SaaS as quickly as possible and will provide notice, to the extent possible, as to the estimated recovery time.

Administration – GitLab is responsible for debugging and resolving application problems, including problems between Dedicated SaaS components of the system. GitLab performs all installation of Dedicated SaaS and configures all hardware and Dedicated SaaS to perform optimally with those products. GitLab uses monitoring information to ensure that the system performs as planned. GitLab provides experienced database administration support for Dedicated SaaS. GitLab will install new versions and updates to databases associated with Dedicated SaaS. GitLab is responsible for maintaining the integrity of the database. GitLab will continually monitor system, application, and database performance and retune these components as necessary to provide optimal performance. GitLab will lead and conduct recovery efforts in the event of a system or component failure that necessitates data restoration.

Reasonable Access - Customer agrees GitLab may reasonably access Customer's underlying Dedicated SaaS infrastructure to alleviate: (1) Downtime, (2) Emergency Events, or (3) other issues that may not rise to the level of severity of (1) and (2), above, but which requires GitLab's reasonable access to alleviate such issues through Unscheduled System Maintenance. GitLab will use commercially reasonable efforts to provide Customer prior notice. By way of example only, direct access to Customer's underlying infrastructure may include, but not be limited to, GitLab connecting to Customer's Dedicated SaaS Kubernetes cluster.

Recovery Plan - GitLab will institute a recovery plan for complete or partial outages of Dedicated SaaS ("Recovery Plan"), establishing, among other things, a Recovery Point Objective ("RPO") and Recovery Time Objective ("RTO"). The Recovery Plan is available at https://about.gitlab.com/handbook/engineering/infrastructure/team/gitlab-dedicated/slas/, as updated from time to time.

Bring Your Own Key or BYOK – BYOK is the use of Customer encryption keys ("Encryption Keys"), which will reside in Customer's applicable cloud hosting provider account. BYOK ensures that Customer Content is encrypted at rest using encryption keys which customer controls. Customer may enable the BYOK feature in its Dedicated SaaS instance. Further information and policies related to the BYOK feature are available at https://docs.gitlab.com/ee/administration/dedicated/#encrypted-data-at-rest-byok.

If Customer elects to enable the BYOK features for its Dedicated SaaS instance, the following additional terms apply:

Customer acknowledges and agrees that certain risks are inherent in managing its Encryption Keys while using the BYOK feature, such as data loss and inability to access its Dedicated SaaS instance. Customer assumes all risks associated with managing its Encryption Keys via the BYOK feature. If Customer deletes, loses access to, or otherwise revokes GitLab's access to the Encryption Keys ("Encryption Key Failure"), GitLab disclaims all liability under this Agreement for any Customer claim, including but not limited to claims for material breach, indemnification, Downtime Credits, or loss of Customer Content.

NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT, INCLUDING BUT NOT LIMITED TO SECTIONS 10 (INDEMNIFICATION) AND 11 (LIMITATION OF LIABILITY), GITLAB SHALL HAVE NO INDEMNIFICATION OBLIGATIONS OR LIABILITY OF ANY TYPE UNDER THIS AGREEMENT IF AN ENCRYPTION KEY FAILURE OCCURS. IF THE FOREGOING EXCLUSION OF LIABILITY IS NOT ENFORCEABLE UNDER APPLICABLE LAW, GITLAB'S LIABILITY SHALL NOT EXCEED $1,000.00 USD.

**6. INCIDENT REPORTING**

In the event of an Incident, GitLab will engage the services of support teams, including hardware and software teams, when necessary, to resolve the Incident. To the extent required, GitLab will assess the impact of the Incident on System Availability and make available status reports regarding it to Customer. Once an Incident report covering the Incident has been completed, GitLab will provide an Incident report to Customer upon request.

**7. SUSPENSION OF SERVICE**

GitLab reserves the right to suspend service to the Dedicated SaaS if i) Customer exceeds set application limits as set forth on GitLab's Website or as documented on an applicable Order Form, or (ii) requests or usage deemed malicious in nature is identified to be sourced from Customer accounts, personnel, or systems.

## APPENDIX 3 - Professional Services

With respect to Customer's purchase of Professional Services (as defined below), the following terms will apply.

**1. DEFINITIONS**

"**Change Order**" means any change to an SOW or Order Form, as applicable, as described in Section 2.3 below.

"**Developments**" means Improvements to GitLab's Pre-Existing Work, new technology, written materials, or other deliverables under this Appendix 3, but excluding any Pre-Existing Work.

"**Improvements**" means all modifications and derivative works to Pre-Existing Works resulting from the Professional Services contemplated by this Appendix 3.

"**Order Form**" as defined in the Agreement will be updated to include an ordering document which contains (i) the description of the Professional Services being purchased, from the (a) Professional Services Catalog, (b) Success Tiers Catalog, or (c) such other service catalogs as made available by GitLab from time to time; and (ii) applicable fees, payment terms and other transaction details sold on either a time and materials basis for specified rates, or for a fixed fee as applicable.

"**Pre-Existing Work**" means all rights, title and interest in and to a party's technology and Confidential Information, including all intellectual property rights imbued to a party as of the Effective Date of this Appendix 3, or as applicable, the effective date of any SOW or Order Form.

**"Professional Services"** means GitLab services offerings which may, without limitation, migration implementation, configuration, consulting, dedicated engineering services, training services, or Success Tiers, as set forth in an applicable SOW or Order Form.

"**Professional Services Catalog**" means the predefined scope, level of effort and deliverables for certain Professional Services, as set forth in the corresponding service name found at https://about.gitlab.com/professional-services/catalog/.

"**SOW**" means a written statement of work executed by GitLab and Customer describing Professional Services to be provided hereunder setting forth the time and materials-based objectives (unless otherwise stated as a fixed-fee) including, without limitation, project-specific activities and estimated level of effort. A SOW may be entered into, or incorporated within an Order Form, by and between Customer and GitLab, any GitLab Affiliate, or an Authorized Partner.

"**Success Tiers**" means GitLab success offerings not otherwise provided as or with Software, Supplemental Services, or Professional Services, which may include, without limitation, enhanced technical support or awareness, adoption, usage, and performance offerings, purchased separately by Customer to improve its use and adoption of Software or Supplemental Services, as set forth in an applicable SOW or Order Form.

"**Success Tiers Catalog**" means the predefined scope, level of effort, and deliverables for certain Success Tiers, as set forth in the corresponding tier name found at https://about.gitlab.com/services.

## 2. PROFESSIONAL SERVICES; PAYMENT OF FEES

**2.1.** GitLab will provide to Customer the Professional Services for the Fees specified in an executed Order Form or SOW. For the avoidance of doubt, in the event Customer purchases Professional Services from an Authorized Partner: (i) GitLab's obligations to Customer with regard to any Professional Services hereunder will be limited to this Appendix 3 unless otherwise explicitly agreed to in writing between Customer and GitLab; and (ii) the provisions of Section 6 (Payment of Fees) of the Agreement will not apply as all terms of payment will be directly as between Customer and the Authorized Partner.

**2.2.** Fees for the Professional Services will be calculated on a time and materials or fixed fee basis, as set forth in a mutually agreed Order Form or SOW. In addition to Fees, Customer will reimburse GitLab for Customer approved expenses reasonably incurred in the performance of Professional Services including meals, transportation, overnight accommodations, and any materials purchased for Customer's benefit (charged at cost) (collectively, "Expenses"), if applicable. GitLab will provide valid receipts and other reasonable documentation of such Expenses to Customer upon request and will invoice directly for any such Expenses in addition to the Fees. All Professional Services purchased are purchased separately from the Software and all references to "Order Form" or "SOW" herein will not apply in any way to any Software. GitLab will invoice Customer for Professional Services as rendered on a time and materials basis, unless provided under a fixed fee arrangement, in which case any fixed fee Professional Services, as applicable, will be paid up-front in full and will be non-cancellable.

**2.3.** Customer acknowledges that it may need to purchase additional Professional Services, or approve additional Expenses, if such Professional Services are not completed within any estimated time frames as presented within an Order Form or SOW. If this event occurs or if the parties desire to make changes to an Order Form or SOW during the engagement to address changes in scope or cost, the parties will complete and execute a Change Order. Upon the parties' mutual execution of a Change Order, it will be deemed incorporated by reference in the applicable SOW or in the absence of an SOW, within the Order Form.

**2.4.** GitLab may provide Professional Services through its third-party contractors. GitLab will remain responsible for such contractor's performance pursuant to this Agreement or as otherwise agreed with Customer in writing.

## 3. CUSTOMER COOPERATION

**3.1.** Customer will cooperate with GitLab to facilitate the performance of the Professional Services, which will include, but not be limited, to the following: (i) assigning a project manager with the requisite skills and training to serve as Customer's primary point of contact; (ii) allocating sufficient resources to ensure Customer's ability to meet its obligations; (iii) establishing the overall project direction, including assigning and managing the Customer's project personnel team; and (iv) providing GitLab with, or access to, such facilities (if applicable), equipment and support as are reasonably necessary for GitLab to provide Professional Services, including remote access to the hardware and systems software configuration on which GitLab supports use of the Software licensed by GitLab to Customer.

## 4. TERM AND TERMINATION

**4.1.** This Appendix 3 commences on the Effective Date and continues until the Agreement is terminated in accordance with Section 4 of the Agreement or as otherwise set forth in this Appendix 3. Subject to Section 4.3 of the Agreement, any termination of the Agreement, this Appendix 3 or any SOW, Order Form or Change Order will not entitle Customer to any credit or refund for amounts due and payable as of the date of termination. Notwithstanding the foregoing, either Party may terminate an SOW upon fifteen (15) days prior written notice, provided that Customer will remain responsible for all Fees due and owing for Professional Services delivered prior to the effective date of termination, and further provided, Customer will not be entitled to any credit or refund as the result of said termination. GitLab may (at its sole discretion) suspend delivering Professional Service if Customer breaches the terms of Section 2 (Professional Services; Payment of Fees) until such breach is remedied.

## 5. PROPRIETARY RIGHTS

**5.1.** Each party will retain all rights, title and interest in their Pre-Existing Works. Except as explicitly set forth herein, each party reserves all intellectual property rights not expressly granted to the other party, and no right, title or interest in a party's Pre-Existing Works are transferred to the other party. Further, this Appendix 3 does not contemplate Professional Services for the provision of any Improvements to Customer's Pre-Existing Works, and any such deliverable will be subject to separate terms and conditions as to be mutually and explicitly identified and agreed between the parties in a fully executed SOW or other form of written agreement.

**5.2.** To the extent applicable, Customer hereby grants GitLab a non-transferable, non-exclusive, world-wide and royalty free license to use Customer's Pre-Existing Works necessary to provide the Professional Services under this Appendix 3. To the extent GitLab PreExisting Works or Developments are incorporated into the Professional Services, such GitLab Pre-Existing Works and Developments are provided to Customer in a non-transferable, non-exclusive, world-wide and royalty free license to use solely for Customer's internal business purposes subject to the Agreement, and expressly conditioned on Customer's compliance with the terms of the Agreement. Notwithstanding the foregoing, Customer will own the portion of any deliverable(s) provided to Customer in tangible form consisting of written reports, analyses, architecture diagrams, project plans and similar working documents.

**5.3.** For the avoidance of doubt, GitLab is not restricted from developing, implementing, marketing or selling services or deliverables for other customers or projects that are similar to the Professional Services or deliverables provided under this Appendix 3. Further, any Developments and/or Feedback Materials resulting from the provision of the Professional Services hereunder will be owned by GitLab and Customer will execute and deliver to GitLab any documents reasonably necessary to vest in GitLab all right, title and interest therein subject always to the terms of any applicable open source license.

**5.4.** Any use of Software by Customer will be governed by the Agreement. Customer agrees that its purchase of Professional Services is not contingent on: (i) the delivery of any future Software functionality or features, other than any deliverables as set forth in the applicable SOW; or (ii) on any oral or written public comments by GitLab regarding future Software functionality or features.

## 6. LIMITED WARRANTY

**6.1.** GitLab represents and warrants that its provision of Professional Services under an SOW or Order Form will be rendered in a professional and workmanlike manner. If GitLab fails to meet the foregoing warranty, upon Customer's written notice, within ninety (90) days after completion of the applicable Professional Services, GitLab will, at its sole option and expense either: (i) re-perform and correct the nonconforming Professional Services within thirty (30) days; or (ii) provide a plan for correcting the nonconforming Professional Services within such thirty (30) day period. If the nonconforming Professional Services are not corrected, or if a reasonably acceptable plan for correcting them is not established during such period, Customer may terminate this Appendix 3, or the respective SOW or Order Form, and receive a pro-rata refund for any pre-paid, unused portion of the Professional Services. The foregoing represents Customer's sole and exclusive remedy for a breach of this Section 6.1

**6.2.** The warranty in this Section 6 is void to the extent caused by Customer's: (i) alteration or modification of the Professional Services not otherwise directed by GitLab, or its authorized representatives, in writing; (ii) failure to meet: (a) the minimum system requirements as made available by GitLab including those set forth here:

https://docs.gitlab.com/ee/install/requirements.html; or (b) its obligations set forth in this Appendix 3, or an Order Form or SOW, including, without limitation, those set forth in Section 3 (Customer Cooperation) above, to enable the provision of the Professional Services.

**6.3.** WARRANTY DISCLAIMER. SECTION 6.1 SETS FORTH GITLAB'S EXCLUSIVE WARRANTY WITH REGARD TO THE PROFESSIONAL SERVICES, AND IS IN LIEU OF ALL OTHER WARRANTIES. GITLAB DOES NOT MAKE ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, GITLAB SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

**APPENDIX 4: AI Functionality Terms**

With respect to Customer's purchase and/or use of AI Functionality (as defined below), the following terms will apply:

**1. DEFINITIONS**

1.1. "AI Functionality" means features developed by GitLab and provided in the Software, or Supplemental Services purchased separately, based on artificial intelligence (including machine learning) technologies ("AI") exclusive of any Customer Models or GitLab Models powering the AI Functionality. AI Functionality may produce Output or conduct actions ("Actions") in response to Input.

1.2. "Customer Models" means AI models powering AI Functionality which, irrespective of the source from which they are obtained, are (i) hosted by, or on behalf of, Customer, and (ii) listed as available for use with AI Functionality and implemented consistent with the Documentation.

1.3. "DPA" means the GitLab Data Processing Addendum and Standard Contractual Clauses available at https://handbook.gitlab.com/handbook/legal/data-processing-agreement/, or such other written data processing addendum between the parties.

1.4. "GitLab Models" means AI models powering AI Functionality which are hosted by GitLab, or by a third party listed as a GitLab sub-processor of GitLab as listed on the Website.

1.5. "Input" means (i) input provided by Customer to AI Functionality and (ii) supporting Customer Content processed by AI Functionality in order to generate Output.

1.6. "Output" means code, natural language, and other data generated by AI Functionality.

1.7. "Agreement" means the current GitLab subscription agreement available at https://about.gitlab.com/terms/, or such other written agreement between the parties governing Customer's use of Software.

**2. SCOPE OF USE**

2.1. Subject to Clause 2.2 below, these Terms, along with the Agreement and the DPA, govern Customer's access to and use of AI Functionality and GitLab Models. These Terms are incorporated into and form part of the Agreement.

2.2. GitLab will have no indemnification obligation nor liability of any type with respect to (i) Customer Models, and (ii) Output generated or Actions conducted by AI Functionality powered by Customer Models, unless such exclusion of liability is not enforceable under applicable law, in which case GitLab's liability will not exceed $1,000.00USD.

2.3. In its use of AI Functionality, Customer may transmit Personal Data to GitLab as part of Input (defined above). To the extent Customer's use of AI Functionality powered by GitLab Models involves the processing of Personal Data, Customer's obligations as a Controller under the DPA will apply. Any sub-processors used to provide AI Functionality powered by GitLab Models will be listed at https://about.gitlab.com/privacy/subprocessors/ and all notifications of updates to that list will be done in accordance with Section 14 of the DPA.

2.4. Customer represents and warrants that it has obtained all necessary rights, approvals, and consents for its use of Input. For purposes of these Terms, both Input and Output constitute additional Customer Content as that term is defined in the Agreement. Customer will retain all ownership of Customer Content, as permitted under applicable law.

**3. RESTRICTIONS**

3.1. Customer's use of AI Functionality will comply with the Acceptable Use Policy available at https://about.gitlab.com/terms/#current-terms-of-use.

3.2. Notwithstanding anything to the contrary in these Terms, Customer acknowledges and agrees that (a) AI Functionality may generate the same, or similar, output for GitLab or other third-party end users (e.g., customers, partners), and (b) Customer has no claim of right, title, or interest against GitLab or third-party end users to the extent such claim relates to the same, or similar output generated for GitLab or other third-party end users.

3.3. Customer represents and warrants that it will not use AI Functionality to create, train, or improve (directly or indirectly) a similar or competing foundational or large language model or other generative artificial intelligence service that competes with the provider of the applicable GitLab Model or Customer Model.
3.4. Customer represents and warrants that it will not reverse engineer, extract, or discover the data, models, model weights, algorithms, safety features, or operation of the GitLab Models or Customer Models.

**4. ADDITIONAL DISCLAIMERS**

4.1. Customer acknowledges and agrees that (a) Output, its use, and Actions may be unreliable, insecure, inaccurate, or offensive, (b) Customer will evaluate all Output and Actions before relying on, or making use of, such Output or Actions, (c) Customer is responsible for ensuring any Output incorporated into Customer intellectual property complies with third-party intellectual property rights, and (d) AI Functionality and its Output and Actions are not designed for or intended to be used for meeting Customer's compliance with applicable laws or regulatory obligations.

4.2. GitLab is not responsible for the availability or accuracy of the products or services of any third-party provider of GitLab Models.

**5. AI INDEMNIFICATION, LIMITATION OF LIABILITY**

5.1. Except as otherwise provided in this Section 5, the applicable provisions of the Agreement will govern each party's indemnification obligations and limitation of liability with regard to Customer's use of AI Functionality. GitLab's obligations under Section 10.1 of the Agreement will also apply to Customer Claims related to Output generated by AI Functionality powered by GitLab Models ("Output Claim"). GitLab will not have any obligations under Section 10.1 of the Agreement with regard to an Output Claim if (a) AI Functionality is provided as Free Software or (b) the Output is (i) modified by Customer, (ii) generated in response to Input that Customer does not have a valid right to use, (iii) combined with other products, processes, or materials, or (iv) known, or should have been known, by Customer to infringe or otherwise misappropriate a third party's intellectual property rights. Customer's obligations under Section 10.2 of the Agreement will only apply to modified Output.

5.2. Subject to Section 5.1 above, GitLab will be responsible for the costs and fees associated with the defense of an Output Claim. GitLab will retain sole control over the defense and settlement of an Output Claim, including the selection of counsel, provided Customer may participate in and observe the proceedings at its own cost and expense with counsel of its own choosing. GitLab will not settle any Output Claim that results in a finding of liability or fault with regard to Customer.

**6. TERM AND TERMINATION**

These Terms will commence upon the Effective Date and will automatically expire upon (a) expiration or termination of the Agreement, or (b) expiration or termination of the underlying Subscription to AI Functionality. The parties may terminate these Terms as provided in the Agreement. Upon expiration or termination of these Terms, Customer will immediately discontinue all use of the AI Functionality. The rights and obligations of these Terms which by their nature are intended to survive termination or expiration of these Terms will survive.

**7. MISCELLANEOUS**

Capitalized terms used but not defined in these Terms will have the meaning in the Agreement or DPA. Except as provided in these Terms, the Agreement remains in full force and effect and governs Customer's access to and use of GitLab's Software. To the extent of any conflict or inconsistency between these Terms and the Agreement, these Terms will control.

## SPECIAL TERM 2 – WORK DESCRIPTION

# Description of Work

| | |
|---|---|
| Effective Date | Effective upon date of last document signatory |
| Version | V1.2.1 |
| DOW # | 2127 |
| Customer's Name | His Majesty's Revenue and Customs ("Customer") |
| Customer Contact | HMRC |
| GitLab Contact | [redacted] |
| GitLab Utilization of Subcontractor (if applicable) | If a partner is utilized for subcontracting services please see the applicable list of subcontractors / subprocessors here: https://about.gitlab.com/privacy/subprocessors/#professional-servicessub-processors<br>If the supplier advises the requirement is to be fulfilled via a subcontracted party, then depending on the engagement route and IR35 status, confirmation will be required on the requirement to issue a Status Determination Statement before engagement commences. |

# 1. DESCRIPTION AND AUTHORIZATION

## A. Executive Summary

HMRC has requested a Services Framework from GitLab Professional Services that will enable Enterprise Cloud Services (“ECS”) and other Customer Groups (“CG”) to select and schedule activities aligned to migrations onto, and then full adoption of a new GitLab Dedicated Platform.

This DOW has three main description sections.

DOW Section 2: Initial recommendation for migrating ECS onto Dedicated Platform:

A high-level description of the initial Project Services and Activities that GitLab Professional Services recommends in Year One.

DOW Appendix A: Activities Full Description

Is a low-level description of the aligned Professional Services and Education Activities. They are provided as Exhibits within the Appendix, in the following order.

A. Residency Services
B. GitLab to GitLab system data sync (e.g. GEO) Migration Services
C. API Based (e.g. Congregate) Migration Services
D. GitLab Platform Adoption Services
E. GitLab Education Services

Examples for A|B|C (above) have been indicated in days’ Effort Allowance. Other Educational Milestone based Activities are also described. These can be drawn down from the Framework under a zero dollar Change Order. GitLab will manage the Change Order process for Customer Group when requested.

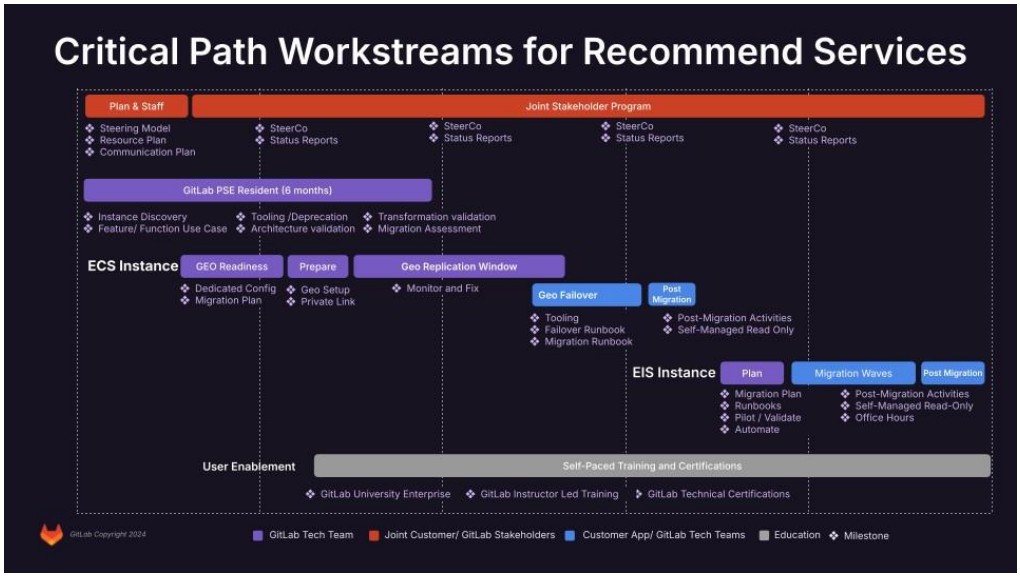
DOW Appendix C: Description of Work Template

Template DOW to be used by GitLab Professional Services and Customer Groups as an Engagement Scope Agreement document.

The total three year Effort Allowances included within this DOW are found in Section 4.A. Effort Allowances and allocation of Effort Allowances will follow the process described in Section 4.C. Requesting, Approval and Scheduling Framework Activities

## 2. INITIAL RECOMMENDATION FOR MIGRATING ECS ONTO DEDICATED PLATFORM - SUBJECT TO TECHNICAL DISCOVERY

GitLab recommends the initial project activities and teaming.




1. Provision GitLab Dedicated environment and onboard core team
2. Provide GitLab University Enterprise and Certifications to establish foundational knowledge of GitLab capabilities
3. Co-design a consolidation strategy for HMRC instances, including org/group structure, user accounts, migration approach, and developer experience

4. Upgrade self-managed instances before migration (should be within 2 minor versions of destination)
5. Clean up repos before migration
6. Build the Migration Plan
7. Scale enablement for app teams with self-paced training and migration runbooks to guide pre and post migration activities
8. ECS Migrations

a. Geo-based migration for ECS instance (must be done first)

9. Follow on with EIS other Customer Group migrations

a. Automated (Congregate) migration waves for EIS instance
b. Automated (Congregate) migration waves for N+ instance(s) 10. Deprecate self-managed instances, when ready

# 3. PROJECT ASSUMPTIONS

## A. Scheduling & Work Structure

When executing project activities;

1. Service Delivery:
    a. All work will be performed remotely (no travel authorized) unless mutually agreed upon
    b. Standard hours are 9am-5pm Monday-Friday in mutually agreed-upon time zone
    c. Non-standard hours require 10 business days advance notice and mutual agreement
    d. Work will run contiguously unless explicitly stated otherwise 2. GitLab Team Availability:

a. Delivery teams follow official government holidays of service delivery location
b. Minimum weekly commitment of 40 hours of work required
c. Project ceremonies must include full working team or delegates with decision authority 3. Schedule Changes & Delays:

a. Delays over five business days due to customer readiness may result in suspended delivery, in which case Customer shall bear the additional cost of restarting the project
b. Schedule modifications based on changes in understood scope as laid out in this document after the delivery of the project plan will require a Change Order and may incur additional fees
c. The customer must provide 10 days' notice for rescheduling/cancellation of project kickoff date

4. Mobilisation

a. After identification of need, selection of Activity and approval from the ECS Governance team, a Standard mobilisation time of 4 working weeks applies. Mobilisation times can be improved with

forward planning and regular engagement between GitLab Engagement Manager/ Program Manager and ECS Governance team.

## B. Technical & Project Scope

1. Technical Constraints:

a. Solutions based on GitLab version features available at contract execution date
b. Project management will use private gitlab.com project for collaboration
c. GitLab provides web conference URLs for all ceremonies
i. Customer responsible for ensuring appropriate distribution to their resources
d. There are two migration approaches for Dedicated, GEO and Congregate, these are the initial decision points.

| **Decision Factor** | **GEO Migration** | **Congregate Migration** |
|---|---|---|
| Source Platform Compatibility | Only GitLab Self Managed | Supports all platforms (GitLab.com, GitHub.com, GitHub enterprise Bitbucket server, Bitbucket cloud, GitLab Self-Managed, Azure DevOps Repos) |
| Connectivity | Network connectivity to a customer-managed database replica | Ability to install VM in customer networks / premises with network connection to source and destination systems |
| Job Artifact Migration | Supported | Not Supported |

2. Access Requirements:

a. The customer must provide system administrator access where needed
b. The customer responsible for acquiring/managing all third-party product licenses
c. The customer must handle internal software installation and usage approvals

# C. Customer Responsibilities

1. Senior Customer Stakeholder

a. ECS ALM are identified as overall Dedicated GitLab Platform Owner
b. Each Customer Group will have a sub Platform/Product Owner
c. Responsible for Customer representation within program steering committee
d. Will attend and support the activities for regular steering committee meetings
e. Acts as Senior escalation point for GitLab
f. Leads initial introductions for GitLab team into Customer Groups e.g. ECS, EIS, CDS CDG etc.

2. Customer Project Management:

a. Responsible for customer program and resource management
b. Manage the engagement and availability of personnel with appropriate skills, access, and decision-making authority
c. Must provide and maintain access to accurate technical documentation in regard to the Customer’s environments, processes, and requirements.
d. Drives customer readiness and resolution of blockers to maintain the ongoing delivery velocity of the project.
e. Responsible for coordinating maintenance windows required to transition.

3. Resource Availability:

a. GitLab will provide 10 working days notice in advance to Customer when requesting skilled resources.
b. Must provide direct contact with key personnel (program lead, users, admins, dev/ops teams)
c. Must provide subject matter experts for technical discussions

i. The Customer's failure to meet obligations impacts GitLab's ability to perform services as estimated in this agreement. Delays resulting from Customer readiness will trigger a change management process that will incur additional cost.

4. Customer Technical Responsibilities

a. Depending on the migration type, the Customer will need to provide access to a replica database instance for GEO migration or for congregate migrations they will need to provide a VM in their network from which we will carry out the migration.

5. Onboarding Support

a. Customer responsible for providing clear guidance for onboarding to the Customer environment, including Laptop provisioning, VPN access, System entitlements, and any required training. Extended Onboarding Activities will need to be mutually agreed upon and may draw down from total T&M hours.

b. Where Security Clearance is necessary, the Customer team will work with GitLab Professional Services to enable suitable candidates with Security Clearance requirements. The Customer team will provide a list of suitability requirements.

D. Joint Activity Management Responsibilities and Tasks

1. Both GitLab and Customer Project Leads will ensure the following responsibilities and tasks are met as are reasonably applicable to the Professional Services being performed:
2. Coordinate, schedule and monitor all resources and activities related to the Professional Services described in this DOW.
3. Coordinate and monitor all project change process activities related to the Professional Services described in this DOW.
4. Act as the focal points for communications between GitLab and Customer during the provision of all Professional Services described in this DOW.
5. Attend Customer and GitLab status meetings, as applicable.
6. Upon becoming aware of a situation which may delay, or threatens to delay, the timely performance of this DOW, promptly communicate this information to the Project Manager who is not aware.

# 4. SCHEDULE AND EFFORT ALLOWANCES

Activities outlined in this Description of Work are scheduled to commence two calendar weeks not to exceed six weeks post DOW execution with a mobilisation meeting in which the parties will review the outlined scope, dependencies, and resources requirements and establish a refinement and roadmap build for the Professional Services engagement cadence.

Subsequent to the mobilisation meeting a schedule of activities will outline the most effective and efficient approach to complete the estimated scope.

In the event Customer Group needs to reschedule or cancel the Professional Services engagement, Customer Group shall provide GitLab with ten (10) business days' prior written notice (email shall suffice).

If Customer Group fails to provide such notice, Customer Group shall pay GitLab's costs directly associated with rescheduling the engagement.

# A. Effort Allowances

Customer acknowledges that they may need to purchase additional Professional Services if the migration to Dedicated Platform is unable to be completed within the Effort Allowances. Any additional Professional Services or scope changes will be documented in the form of a new DOW or Change Order executed by the parties' authorized representatives before GitLab will proceed.

| Effort Allowance | **Quantity in Hours** | **Release Date** |
|---|---|---|
| Year One | 2,424 | Commencement of Dedicated Contract |
| Year Two | 1,212 | Annual Renewal Year Two |
| Year Three | 1,212 | Annual Renewal Year Three |

A target of 50% of the Year One value of the Effort Allowance is to be consumed within the first twelve months and the remaining value of the Year One Effort Allowance is targeted to be executed in Year Two.

All Professional Services pursuant to this DOW but not completed or delivered within twenty-four (24) months of the Effort Allowance Release Date, will result in termination of such Professional Services, in which case; (i) no refund or credit shall be due for any pre-paid amounts. Both parties may extend the agreement via mutually signed Change Order.

1. In performance of the Professional Services described, GitLab shall perform the project activities listed in this DOW utilising the pre-billed fixed fee amounts detailed in the Effort Allowances.
2. GitLab will:

a. Provide monthly budget utilization reports aligned with the project plan
b. Alert Customer promptly of any potential budget risks
c. Not exceed the estimated days without Customer's written approval

d. Not commence a new work activity without an approved Work Authorisation from ECS Governance team

3. Additional time and fees may be required if:

a. Material changes occur to project scope or complexity after plan acceptance

b. Key assumptions or requirements are not met

c. Any changes requiring additional days must be approved via Change Order before work begins.

4. Travel & Expense

a. All reasonable travel expenses incurred by GitLab personnel in performance of the Services under this DOW shall be reimbursed by Customer at cost, including but not limited to airfare, ground transportation, lodging, and meals. Travel expenses require Customer's prior written approval for any trip with all reasonable costings outlined ahead of time for approval by the Customer. All expenses must be supported by original receipts and submitted within [30] days of incurrence.

b. The GitLab Professional Services team will deliver services subject to any reasonable travel and expense policy provided by Customer prior to project kickoff. If the travel and expense policy is not provided in a timely manner, or the Customer does not have a travel policy for contractors, then the GitLab Professional Services team will deliver services subject to GitLab's own internal travel and expense policies.

## B. Changes to Scope

Will require;

1. Written identification from GitLab or written request from Customer
2. GitLab estimate of time and cost to complete
3. Mutual agreement via Change Order

# C. Requesting, Approval and Scheduling Framework Activities

1. ECS Governance team will make requests to either GitLab scoping representative (Engagement Manager or GitLab Program/Project Manager) to engage with a Customer Group.
2. GitLab scoping representative will engage in a discovery with Customer Group and identify their Activity needs.
3. GitLab scoping representative will validate and provide back to Customer Group an Activity requirement in the form of a Work Authorisation document (see Appendix B).
4. Customer Group will either iterate with GitLab scoping representative or pass Work Authorisation directly to ECS Governance team for approval.

5. ECS Governance team will approve/iterate/decline Work Authorisation request.
6. Once approved, ECS Governance team will advise GitLab scoping representative who will then send approved Work Authorisation to GitLab delivery team for team mobilisation and activity execution.

Note: A Work Authorisation is only deemed as approved for mobilisation and execution when fully executed by both GitLab and ECS signatories.

Note: Work Authorisations can be approved but may not be scheduled if the remaining budget is not sufficient to cover the days required to execute.

# 5. Payment

Invoices shall be due and payable via the terms of the AWS Marketplace through which Customer shall accept the terms of this DOW. All invoices shall be provided and paid via AWS as the marketplace partner facilitating the sale of Professional Services to Customer via the AWS Marketplace and the terms and conditions as between GitLab and AWS.

The fees set forth on this DOW are exclusive of all taxes, levies, or duties imposed by taxing authorities and the Customer shall be responsible for payment of any such taxes, levies or duties, excluding only taxes based solely on GitLab's net income. Accurate sales tax will be added to invoices when applicable.

## A. Acceptance of Fixed Fee Services (Education)

**Training**: To the extent Customer has purchased training, acceptance will be deemed to have occurred upon GitLab’s confirmation of the list of attendees.

**Technical Certification redemption codes**: To the extent Customer has purchased Certification redemption codes, acceptance will be deemed to have occurred upon GitLab’s delivery of redemption codes via email.

Note: Examples of GitLab Education offerings are found in Appendix A: Activities - Full Description , Exhibit E: GitLab Education Services.

Throughout the project, GitLab will collaborate with Customer through agile ceremonies, through which work will be prioritized, delivered and reviewed on a continuous basis. As such, once the final sprint completes, the project is considered complete and delivered.

# 6. DOW ACCEPTANCE

This DOW may be withdrawn by GitLab if not accepted by Customer on or before September 30th, 2025.

The applicable terms and conditions related to the GitLab's offer to provide the GitLab Professional Services stated herein shall be agreed to and accepted by Customer by virtue of accepting or otherwise clicking to accept the related private offer within the AWS Marketplace.

Unless otherwise agreed to between the parties in writing, by accepting the purchase of the Professional Services via private offer in the AWS Marketplace, Customer unconditionally agrees to be bound by and a party to the terms of this DOW, the Contract between the parties, including the Professional Services Annex to Special Terms 1, and further agrees that all terms stated within a purchase order, or other similar document, shall be null and void and are expressly rejected.

# APPENDIX A : ACTIVITIES - FULL DESCRIPTION

Exhibit A : Residency Services

| Resident Engineer ( Flexible number of months) |
|---|

**Included**

- Supporting GitLab application administration
- answering end user questions and addressing issues.
- troubleshooting system outages and possible performance issues.
- provisioning users, groups and projects and managing permissions.
- reviewing workflow strategies, patterns and integrations and making best practices recommendations.
- troubleshooting current integrations as needed.
- updating Customer GitLab documentation as needed.
- upgrading and maintaining GitLab instance, reviewing maintenance practices, and making recommendations for improvements.
- conducting GitLab health check and defining architecture changes to scale GitLab instance.
- Consulting on GitLab configuration and rollout approach
- defining group, subgroup and project organization.

- advising on appropriate use of epics, milestones, labels, and roadmap for portfolio and project planning and tracking.
- establishing appropriate workflows, including branching strategy, code review practices, and merge request approval rules to satisfy compliance needs.
- Advising on implementation best practices for optimal infrastructure setup and performance.
- providing guidance on runner fleet setup to support Customer pipelines and performance requirements.
- help achieve desired reference architecture deployment and design.
- Defining migration strategies and patterns that are applicable to Customer's requirements.
- performing manual migrations from source to destination.
- advising on running scripted migration that leverages import/export API or direct transfer.
- Advise on performing back/restore or GEO based migrations.
- performing scripted API based migration at the customer's direction.
- creating migration and troubleshooting documentation
- Devising CI/CD and DevSecOps strategies, patterns, and templates.
- establishing CI patterns for standard application types, including
- troubleshooting pipeline errors and creating end user documentation of root cause and resolution.
- establishing best practices for various deployment types - automated deployments and blue/green deployments.
- creating patterns for deploying AWS lambda functions.
- defining patterns to leverage value stream management and track associated metrics.
- creating templates that introduce SAST, DAST, Container Scanning, and other security scans within standard CI/CD pipelines.
- devising patterns for integrating package and container registries into CI/CD pipelines.
- Creating Runner strategies, patterns, and configuration.
- architecting runner infrastructure to enable DevSecOps pipeline patterns, including defined usage patterns for shared vs. private runners.
- establishing runner configurations, restrictions and tagging.

**Excluded**

- Resident GitLab Engineer shall not provide GitLab training.
- GitLab uses specific training collateral and resources that must be scoped outside of the engagement.
- Resident GitLab Engineer shall not perform activities that don't provide GitLab related value to the Customer.

| **Program Management** |
|---|
| GitLab shall in collaboration with Customer develop a project definition document that serves as a comprehensive project plan that defines:<br>• The timeline, activities, milestones and possible project risks;<br>• The objectives and scope;<br>• The roles and responsibilities of the parties;<br>• The project management process<br>• Communication plan and change control process<br>• GitLab shall, in collaboration with the Customer project manager, monitor project<br>• and report status of budget, issues, timeline, and expenses on a weekly basis. |
| **Assumptions**<br>• Customer responsible for providing context and requirements for work items to be completed by GitLab. This is typically accomplished with the normal Agile work process.<br>• GitLab technical training is outside the scope of this engagement.<br>• GitLab will only work on activities that provide GitLab related value to the Customer.<br>• All work will be performed remotely.<br>• GitLab will work towards achieving the outcomes of each of the activities with the hours allocated, but there is no requirement of completion of said activities or specific deliverables.<br>• The customer agrees to 40 hours of GitLab Professional Services Engineering work and 4 hours of GitLab Project Management time a week, unless an exception is granted.<br>• If an exception is granted, GitLab Project Management time will be adjusted accordingly to ensure 10% allocation via Change Order. |

# Example efforts for Residency Services.

| **Activity Type** | **Activity Name** | **Key Metrics** | **Effort in Days** |
|---|---|---|---|
| **Residency** | **Resident Engineer** | 40 hours / week<br>for<br>6 months | 120 |

Exhibit B : GEO Migration Services

| Dedicated Geo Migration - Data Replication and Sync Monitoring |
|---|
| **Included**<br>• Provide guidance during the configuration and connection of the data sync via Gitlab Geo between the customer primary and secondary deployment.<br>• Monitor syncing progress, flagging and addressing data quality issues.<br>• Address replication across Gitlab data types.<br>• Must provide access to production observability platform gathering logs and statistics about primary GitLab instance.<br>• Run pre-flight checks and create a plan for resolution of any identified issues (DNS / TTLs / Cutover / etc.) |
| **Assumptions**<br>• Customer will maintain a parity of N-2 with Dedicated throughout the replication process of the customer's instance.<br>• Customer will acknowledge that the Dedicated environment cannot pause upgrades, and synchronization will only occur when parity exists between systems. |

| Dedicated Geo Migration - Failover Implementation and Validation |
|---|
| **Included**<br>• Minimize downtime with a pre-planned process for promotion and failover.<br>• Perform geo failover implementation and validation, including failover dry run after sync is accepted.<br>• Create a failover runbook and tooling needed to perform the failover after testing is accepted.<br>• Support team in the execution of the planned failover, including preparation, downtime activities, database migrations, and post-failover support. |

| Dedicated Geo Migration - Migrate from NFS to Object Storage |
|---|
| **Included**<br>• Validate and test object migration to S3 and retrieval |

| Dedicated Geo Migration - Network and Runner Design & Discovery |
|---|

**Included**

- Develop a plan to replicate the identified primary environment on the Gitlab Dedicated architecture leveraging the Gitlab Geo product with an agreed approach to cutover transition.
- Perform technical discovery of current environment and constraints related to leveraging GitLab Geo as a migration tool for the move to dedicated architecture.
- Enumerate integrations, external touchpoints, inbound and outbound traffic (runners, OIDC, VPN, etc.)
- Create a data migration plan for object storage, git, and database replication
- Identify required changes to the current environment to align with desired outcomes with the move to Dedicated architecture.
- Material changes that would exceed the current estimates in this DOW will be discussed and prioritized or amended to this scope via a paid change order.
- Develop GitLab Geo based migration plan with clear:
- Dependencies and requirements
- Risks and mitigations
- Go live process
- Pre and post migration steps
- Final cutover steps
- Review design with AWS account team and GitLab internal teams to identify constraints and optimizations.
- Conduct design review with AWS and GitLab teams
- Identify constraints and needed optimizations
- Networking before-state and after-state design
- Assist with private links and VPC connectivity configuration

| Dedicated Geo Migration - Postgres Read Replica for Dedicated Testing |
|---|

**Included**

- Create an additional PostgreSQL read replica that the GitLab Dedicated team will use as their secondary site database to test connectivity and replication into the Customer deployment account
- Standing up a new PostgreSQL database
- Configuring and starting streaming replication
- Coordinating with GitLab Dedicated for configuration / networking / etc.

| Dedicated Geo Migration - Project Manager |
|---|
| **Included**<br>• Manage the planning, execution, and completion of delivery tasks for the Gitlab team. Serving as the main point of contact throughout delivery to drive collaboration requirements and dependencies across the Gitlab and Customer teams.<br>• Project roadmap, steering committee, and progress reporting<br>• Program planning via delivery criteria definition and acceptance<br>• Communication management<br>• Project management framework and tooling<br>• Risk and dependency management process<br>• Scope change management<br>• Budget consumption reporting |

| Dedicated Geo Migration - Secondary Promotion for Dedicated |
|---|
| **Included**<br>• Minimize customer downtime with a pre-planned process for promotion and failover.<br>• Perform secondary to primary promotion functions. |

| Integration - Guided Support<br>*Help Customer implement integrations using the guided support methodology.* |
|---|
| **Included**<br>• Review documentation on standard integrations.<br>• Build plan to implement standard integrations<br>• Provided guidance to Customer while implementing the integrations. |
| **Assumptions**<br>• Activity 13 will follow the GitLab guided support model. GitLab engineers will follow along and offer direction as Customer engineers perform tasks against their systems and accounts. GitLab engineers will not interact directly with Customer systems nor accounts for this activity. |

| **Deliverables**<br>• Configured integrations for the standard list of GitLab integrations |
|---|

| Integrations - Jira, Jenkins, & SSO<br>*All in one offering to cover standard integrations of Jira, Jenkins, and SSO* |
|---|
| **Included**<br>• Perform discovery functions related to GitLab-Jenkins, GitLab-Jira, and GitLab-SSO integration and expectations.<br>• Configure GitLab-Jenkins, GitLab-Jira, and GitLab-SSO integration.<br>• Explain how users will experience the GitLab-Jenkins, GitLab-Jira, GitLab-SSO integration.<br>• Validate SSO integration by having users of various access levels log in.<br>• Validate Jira integration with a test repo connected to a test Jira project and verify smart commits work. |
| **Assumptions**<br>• The Jenkins integration involves connecting an existing Jenkins instance to GitLab to trigger a Jenkins job when code is pushed to GitLab.<br>• These integration does not include translating or transforming Jenkins pipeline files into GitLab CI.<br>• The Jira integration involves connecting an existing Jira issues or Jira development panel to GitLab.<br>• The SSO integration involves setting up SSO on a GitLab instance. |

# Example efforts for a GEO Migration Services.

| **Activity Type** | **Activity Name** | **Key Metrics** | **Estimated Effort in Days** |
|---|---|---|---|
| Dedicated Geo Migration | Data Replication and Sync Monitoring | Dedicated work duration 24 weeks | 12 |

| | | | |
|---|---|---|---|
| | Failover Implementation and Validation | | 10 |
| | Migrate from NFS to Object Storage | Prep and meeting per SteerCo 8 hours | 5 |
| | Network and Runner Design & Discovery | Program Management Capacity 8 hours/week | 20 |
| | Postgres Read Replica for Dedicated Testing | | 15 |
| | Project Manager | Replication time estimate - 16 weeks | 65 |
| | Secondary Promotion for Dedicated | Replicate fix and monitor 8 hours/week | 5 |
| Integration | Jira, Jenkins, & SSO | 1 day/ standard integration | 3 |

Exhibit C : Congregate Migration Services

| Migration - Automated Migration Plan, Design and Preparation |
|---|
| *Create plan to migrate up to {{max_users}} users, {{max_projects}} GitLab projects, perform a sample migration, inspect the results, and capture required migration automation improvements.* |

**Included**

- Assist Customer in creating a Migration Orchestration Plan with migration timelines.
- Determine which repositories will be used in the sample migration. The selection of repositories should represent the widest use cases possible so that any issues can be identified early.
- Cleanup source instance by removing or archiving all unneeded repositories, branches, artifacts, and/or pipelines.
- Plan out repository migration waves based on project release schedules, dependencies and group or team organization.

- Work with Customer to determine and document group and project conflict resolution strategy.
- Work with Customer to determine and document user conflict resolution strategy.
- Discovery activities will be performed with stakeholders from each of the {{total_portfolios}} portfolios to be migrated.
- Generate base migrations wave file for Customer.
- Advise Customer on how to create a User Migration Change Management Plan to set end users' expectations about their experience during the migration.
- Identify stakeholders for each of the {{total_portfolios}} portfolios to be migrated.
- Work with Customer after sample migrations to identify any missing requirements.
- Create a list of migration automation update requirements.
- Identify the source and GitLab destination Service Accounts that will be used to facilitate the migration.
- Migrate the sample set of projects as described in the Migration Orchestration Plan.

**Assumptions**

- Customer will allow https (443) and/or http (80) (if the source site is insecure) access and interconnectivity between source systems, the destination system, and the migration VM used to conduct the migration to ensure GitLab can effectively use its automated data migration tooling.
- It may be necessary to allow access to additional systems/addresses/ports such as registry ports on GitLab instances (if hosted on other than 443/80), build systems, or other artifact management systems.
- When migrating to GitLab.com, the following IP ranges specified here and hostnames specified here need to be accessible to and from the source instance. Other ranges TBD depending on the source and destination systems.
- This migration will **not** include re-organization of groups or projects.
- Migrations will be limited to the features supported by available migration tooling at the time of signing. Any additional features or custom scripting should be scoped as a separate activity.
- Discovery activities will be performed with stakeholders from each of the {{total_portfolios}} portfolios to be migrated.
- This migration is constrained to {{max_source_systems}}{{source_vcs}} source(s), {{max_users}} users and {{max_projects}} repositories depending on the users, data, source, destination, and environment setup.
- Projects with git repo sizes greater than 5GB will be excluded from the automated migration for non GitLab.com destination migrations.
- If the migration destination is GitLab.com, projects with Git repositories sized between 5GB and 10GB can be migrated using S3. However, projects exceeding 10GB will not be supported.
- User projects will be excluded.
- For migrations from one GitLab instance to another (self-managed and/or GitLab.com), the source and destination instances must be lagging by no more than 2 minor versions.

- The destination GitLab deployment is functioning properly and supported by infrastructure (servers, storage, networking, etc.) sufficient to support the increased project load.
- User conflicts that cannot be resolved with the chosen strategy will be resolved manually by Customer.
- Project conflicts that cannot be resolved with the chosen strategy will be resolved manually by Customer.
- This migration will not include manual data massaging nor custom data massaging automation.
- Customer will provide repository hierarchy information to support the use of GitLab Groups.
- GitLab Professional Services will make use of migration automation software that they have built and maintained to support mass migrations for other customers and follow License guidelines.
- GitLab migration automation will be removed when the engagement completes.
- GitLab engineers will perform the migrations with direct command-line access to the migration automation wherever it may reside.
- Customer will establish services accounts on the source and destination systems as follows:
- Customer will establish a service account on the source system with read-write access to all groups, projects and repositories to be migrated.
- Customer will establish a service account with read-write access on the destination GitLab system.
- Customer will need to provide an instance admin token for any source and destination instance they are responsible for.
- Customer will support Activity with subject matter experts who can:
- Describe success for the migrated users.
- Describe success for the migrated projects.
- Contribute to the organization of project migration waves and
- Provide system administration support.
- The migration will not include any mirroring.
- It's expected that migration automation update requirements will be identified and the migrated projects will have to be removed.

**Deliverables**

- Migration Plan Documents including:
- User Migration Change Management Plan (as necessary).
- User Conflict Resolution Plan (as necessary).
- Group and Project Conflict Resolution Plan (as necessary).
- Migration Waves file.
- Migration Automation Update Requirements.

| Migration - Automated Source Code Migration Execution |
| --- |
| *Create up to {{max_users}} destination GitLab users. Migrate up to {{total_projects}} projects and associated groups from source to GitLab destination.* |
| **Included**<br>• User Migration<br>• Execute the User Migration Plan to arrive at destination GitLab users corresponding to source users.<br>• Inspect the destination GitLab users to ensure they are representative of the source users.<br>• Migration Wave Orchestration and Spot Checks<br>• Implement the updates defined in the Migration Automation Update Requirements.<br>• Execute the Migration Orchestration Plan.<br>• Set the source projects to read-only. |
| **Assumptions**<br>• It may be necessary to re-execute the User Migration Plan after GitLab Automation Adjustment depending on inspection findings.<br>• Customer will support Activity 16 with Source and Destination instance administrator personnel.<br>• While Activity 16 will be performed largely in an asynchronous fashion, it will require sporadic Customer system administrator support.<br>• GitLab best practices are to use variables and avoid URL hard link references.<br>• Customer will be responsible for fixing any hard link references. |
| **Deliverables**<br>• Destination GitLab instance with migrated users, projects and groups. |

| Migration - Manual SCM Migration |
| --- |
| *Plan and execute the migration of users, groups, and GitLab projects and create destination GitLab groups and projects corresponding to source.* |

**Included**

- Create a User Migration Plan to describe the migrated users' experience (emails, cutover timeframe, etc.).
- Identify and validate proper access to the source and GitLab destination systems that will be used during the migration.

- Determine and document project conflict resolution strategy.
- Define 20-user migration waves based on project release schedules, inter-project dependencies and group organization.
- Determine and document user conflict resolution strategy.
- Define 10-project migration waves based on project release schedules, inter-project dependencies and group organization.
- Execute the group and project components of the Migration Orchestration Plan.

**Assumptions**

- This migration is constrained to a certain number of source(s), users, and repositories depending on the users, data, source, destination, and environment setup.
- GitLab instances must be up to date or lagging the current version by no more than 2 minor versions.
- Project and user conflicts that cannot be resolved with the chosen strategies will be resolved by Customer.
- Customer will allow network connectivity between the source and destination systems of the migration.
- For migrations to gitlab.com, it is required that the IP ranges specified here as well as the hostnames specified here must be accessible from the source and destination systems.
- <<Describe success for the migrated users>>
- <<Describe success for the migrated projects>>
- Contribute to the organization of <#> project migration waves.

**Deliverables**

- Migration Plan Document
- User Migration Plan and Migration Orchestration Plan
- Destination GitLab Groups
- Destination GitLab Projects

Migration - User Mapping

*Map placeholder users on GitLab destination to actual users.*

**Included**

- Provide Customer with csv of user mappings to emails on destination instance per toplevel group.
- Gain Customer signoff and validation on csv.
- Map placeholder users on target instance to GitLab Customer users for attribution and membership assignment.

**Assumptions**

- Depending on the authentication method, GitLab may need to configure additional SCIM parameters outside the normal
- Customer may be required to provide additional destination tokens (owner namespace) or provision a user for us in their namespace
- Customer will validate and sign off on csv mapping provided **before** GitLab can complete mapping exercise on destination.
- There are features/steps that should NOT be taken until membership mapping is complete, which can be found in the documentation.
- There can be no restructuring of groups or projects during the migration until after the user mapping is completed.

**Deliverables**

- All desired Customer users are mapped properly on the target instance after accepting membership.

Project Management

*Manage the planning, execution, and completion of the project, ensuring that all deliverables (as applicable) meet Customer expectations. Includes resource allocation, risk management, and coordination between stakeholders to achieve project objectives efficiently, leveraging GitLab collaboration project.*

**Included**

- Agree on a project management methodology with Customer to serve as a comprehensive Project Plan which defines:
- Project roadmap, success criteria metrics, and Communication Plan against the project objectives, scope, timeline, and activities
- The project management framework, cadence, approach, and tooling
- Risk management and change control process
- Project initiation, information gathering and consolidation, and customer expectation setting.
- Facilitate project kick-off, discovery sessions, working sessions (as needed), steering committee meetings (as needed), and Project Closure.
- Create, update and maintain Project Plan.
- Coach Customer Project Manager on best practices in execution of Communication Plan.
- Provide updated status reports and Project Plan documentation to key Customer stakeholders.
- Hold stakeholder steering committee calls (as mutually agreed upon).

**Assumptions**

- Customer is responsible for overall program management activities including but not limited to cross project coordination and identification and management of internal customer stakeholders.
- GitLab and Customer will collaborate on resource alignment through defining roles and responsibilities of the project participants.
- The Customer will collaborate on setting and agreeing to the Communication Plan as an output of the Customer Kickoff and during the initial Discovery Meetings.
- Project management tooling is hosted on a private project on gitlab.com. Customer is expected to collaborate within GitLab using issues, issue boards, milestones and iterations. If Customer is unable to use gitlab.com for collaboration in this way, Customer shall notify GitLab no later than 5 days after contract signature.

**Deliverables**

- Project Plan with clear definitions of done against the project success criteria.
- Status Reports according to the Communication Plan, including burndown reports.

# Example efforts for a small Congregate Migration Service

| Activity Type | Activity Name | Key Metrics | Estimated Effort in Days |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Integration | Jira, Jenkins, & SSO | 1 day/ standard integration | 3 |
| Non GEO Migration | Automated Migration Plan, Design and Preparation | 1 Self Managed Source | 3 |
| | Automated Source Code Migration Execution | 1 Dedicated Destination | 1 |
| | Manual SCM Migration | 500 Users | 1 |
| | User Mapping | | 1 |
| | Project Management | | 2 |
| | | 200 Projects<br>198 Repos <= 5GB<br>2 Projects > 5GB | |

Exhibit D : GitLab Platform Adoption Services

| |
|---|
| CI/CD App Modernization<br>***Embed 1 candidate application with GitLab best CI/CD practices.*** |

**Included**

***Discovery & Kickoff***

- Identify one (1) mutually agreed upon candidate application for CI/CD discovery requirements.
- Pilot team should represent a large portion of the application development processes at your company. The team selected should be innovators and intrinsically motivated to improve the ways of working to increase agility and efficiency.
- Investigate the tech stack and build automation of pilot project.
- Review current customer application CI/CD workflow.
- Understand pilot application's deployment patterns, cloud environments, and constraints (e.g. security, network, firewall, etc.).
- Develop written requirements and validation criteria.
- Document customer goals and objectives (meeting notes sufficient)
- Document concepts and answered questions during the engagement

***Application Pipeline Transition***

- Translate agreed-upon pilot application pipelines from source CI tool into GitLab CI, if they exist, or create new pipelines from scratch for the targeted application.
- These pipelines should be end to end working examples.
- Validate translated pipeline against previously agreed validation criteria
- Document and demonstrate new end to end pipeline with embedded GitLab best practices to Customer.
- Discuss next steps in terms of driving adoption more broadly within the organization.

***Project Management***

- Manage the planning, execution, and completion of delivery tasks for the Gitlab team. Serving as the main point of contact throughout delivery to drive collaboration requirements and dependencies across the Gitlab and Customer teams.
- Project roadmap, steering committee, and progress reporting
- Program planning via delivery criteria definition and acceptance
- Communication management
- Project management framework and tooling
- Risk and dependency management process
- Scope change management
- Budget consumption reporting

**Assumptions**

- Customer will introduce key customer personnel including Executive sponsor(s), Project Manager, Super Users and System Administrator(s), Development, Security, and Operations leaders.
- Customer does not require an air-gap in their GitLab environment, and if so, understands additional configuration may be needed to get a working project example set up in their environment that could be out of scope.
- Customer will support Activity with core project and application team who can discuss:
- Configuration of project structure and permissions.
- Branching strategy workflows.
- Infrastructure as code, environment and secrets management, variable parameterization, and pipeline keywords and rules.
- Integration of 3rd party external CICD tools may adjust scope and cost of Activity.

**Deliverables**

- Documentation of customer goals and objectives (meeting notes sufficient).
- Documentation of the concepts and answered questions during the engagement.
- 1 pilot application GitLab pipelines have end to end CI/CD pipelines and workflows integrated achieving customer vision with GitLab best practices.

DevSecOps App Transformation

*Create 1 model GitLab DevSecOps build-to-deploy security workflow by incorporating GitLab's vast security features into an existing GitLab application.*

**Included**

***Discovery & Kickoff***

- Schedule to meet with the DevOps Platform/Security team to review.
- Identify common tech stacks used by Customer development teams.
- Understand current environment setup and infrastructure/process constraints (e.g. security, network, firewall, etc.).
- Schedule to meet with QA, and security/compliance team SMEs to understand the current security requirements, tool suite, and workflow process.
- Plan delivery of education services (method of delivery as well as content), timeline, and documentation deliverables.
- Identify and gain access to customer team with sample application and inspect code to understand current tech stack, integrations, dependencies, pipeline, etc.
- Identify 1 (one) pilot application to use to build in security pipelines and show off GitLab Ultimate security features.

***Security Pipeline Transition***

- Add and explain merge request approval settings to encourage shift left mindset in security reviews.
- Add all GitLab security scans required to the application pipelines and verify they function correctly.
- Show off security scan job logs and generated artifact from the pipeline view and how the results populate in the UI of a merge request.
- Add workflow rules in pipeline file and any required security scanner configurations to customize how the scans run and when they run based on the customer's preference.
- Showcase SBOM, license information, the GitLab compliance center, and how to set up audit events.
- Show off security dashboard and vulnerability management capabilities within GitLab. ○ Identify vulnerability triage process, metrics over time, vulnerability status, and vulnerability report generation.
- Set up and demonstrate scan execution policies for automation of security pipeline enforcement.
- Set up and demonstrate merge request approval policies to automate additional merge request approval requirements depending on security scanning results.
- If necessary, perform a comparison of customer's existing security tool job outputs to GitLab's scanning solutions to justify using GitLab tools. Otherwise, integrate 3rd party security tools as required.
- Document and record sessions to provide to customer at the end of engagement.

***Project Management***

- Manage the planning, execution, and completion of delivery tasks for the Gitlab team. Serving as the main point of contact throughout delivery to drive collaboration requirements and dependencies across the Gitlab and Customer teams.
- Project roadmap, steering committee, and progress reporting
- Program planning via delivery criteria definition and acceptance
- Communication management
- Project management framework and tooling
- Risk and dependency management process
- Scope change management
- Budget consumption reporting

**Assumptions**

- Customer will introduce key customer personnel including Executive sponsor(s), Project Manager, Super Users and System Administrator(s), Development, Security, and Operations leaders.
- Customer does not require an air-gap in their GitLab environment, and if so, understands additional configuration may be needed to get working project example set up in their environment that could be out of scope.
- Customer will support Activity 4 with subject matter experts who can discuss: ○ GitLab's "shift-left" mindset to enforce security and compliance earlier in the merge approval workflow.
    - GitLab's security scanning solutions. ○ Creation of standardized security policies and how to enforce it across multiple projects.
    - GitLab's security dashboard, vulnerability remediation, and scan result/scan execution policies.
- Integration of several 3rd party security tools may adjust scope and cost of this engagement

**Deliverables**

- Demonstration of a golden DevSecOps pipeline transformation for a pilot application.
- Best practices and recommendations documentation for the Customer's GitLab DevSecOps workflow setup

Exhibit E : GitLab Education Services

| Education - GitLab University Enterprise - Setup, Access, & Content Updates |
|---|

*GitLab will configure, provide access, and deliver quarterly content updates for the GitLab University Enterprise eLearning portal, ensuring a seamless and effective learning experience that drives GitLab adoption and enhances team skills.*

**Included**

- Facilitate access to the GitLab University Enterprise portal using a registration code or Single Sign-On (SSO) setup.
- Ongoing administrative support for minor UI bugs, text edits, access issues, and dashboard configuration updates.

**Assumptions**

- Customer will provide required branding assets, user role definitions, and integration specifications.
- Any integrations or modifications beyond the agreed scope will require a separate change request.
- Customer will assign a primary point of contact for setup coordination and approvals.
- Learners require internet access and a modern web browser (Chrome, Firefox, Safari) excluding Internet Explorer.
- Access is safeguarded with a license code and unique login credentials, requiring a valid email address associated with the customer's company domain.
- Updates are limited to minor content modifications. Major content revisions or new module development will require a separate agreement.
- After the term of this engagement has ended, access to the platform will be autorenewed for a 12 month period unless the Customer has decided to opt out, in which case a 30 day notice of non-renewal (cancellation) is required from the Customer.

**Deliverables**

- Fully configured GitLab University Enterprise platform tailored for Customer with up-todate content

Education - Train-the-Trainer

*Empower customers with the capabilities to deliver GitLab training internally.*

**Included**

***GitLab Standard Training***

- Standard single day (8hr) remote training of Customer's choice by a GitLab certified trainer.

***Consultancy***

- Conduct strategy sessions between GitLab Technical Instructor and Customer about class delivery, maximizing participation, and effectiveness of training, scaling, and developing informative content.
- Discuss trainer skills including:
  - Remote delivery challenges and approaches
  - Common GitLab training pitfalls and challenges
- GitLab Technical Instructor reviews and provides feedback on the curriculum content as the Customer creates it.
- Preparation for co-teaching phase. ***Co-Teach***
- GitLab Technical Instructor and 4 Customer trail blazers jointly deliver newly-created content in a safe environment.

***Consultancy***

- Refine the delivery process for class as needed to optimize learning.
- Customer updates content and training setup, peer-reviewed by a GitLab Technical Instructor.
- Final preparation for customer-led delivery of new content. ***Customer-led Training***
- Customer fully leads and delivers new training to up to 12 attendees, managing content, delivery, and other logistics.
- GitLab Certified Trainer observes the customer-led training and provides any final feedback and/or notes moving forward.

**Assumptions**

- GitLab Technical Instructor will not create customized curriculum content for Customer.
- The train-the-trainer engagement is typically delivered in multiple sessions over several days. All sessions will be agreed in advance with the nominated Project Coordinator.
- Customer will set up their own GitLab training lab environment.
- Train-the-trainer services do not include ongoing access to the GitLab Cloud training environment.
- GitLab will support this activity with a GitLab certified trainer.

**Deliverables**

- GitLab material about effectively delivering remote training.
- 4 Customer trail blazers enabled with knowledge and skills to create and deliver successful training to the rest of their organization.

Education - GitLab with Git Fundamentals Training

*Provide private Instructor-led GitLab with Git Basics Training.*

**Included**

- Provide training for the following focus areas: ○ Explain what GitLab is and why teams use it. ○ Perform basic Git commands for branching, merging, and remote work. ○ Apply fundamental concepts and skills using GitLab within the DevOps lifecycle.

**Assumptions**

- Attendees will have access to Gitlab accounts with Configured runners.
- Attendees must confirm with the training coordinator that all system requirements (https://university.gitlab.com/pages/gitlab-ilt-sysreq/) for the class have been met prior to the class start date.
- Attendees must have access to web browsers other than Internet Explorer.
- Attendees will participate in practice exercises (labs).
- Remote ILT class(es) is delivered in a single day, including a 1-hour break for lunch.
- Remote ILT class(es) may finish early depending on attendee feedback and lab participation.
- Attendees are required to join web conference sessions with cameras enabled to foster interactive sessions.
- Recording and/or distribution of recordings of ILT classes in any way is strictly prohibited unless explicitly provided by GitLab in writing prior to such recording or distribution.
- Training accommodates 12 participants, with a maximum capacity of 15 participants available through the purchase of 3 additional seats.

**Deliverables**

GitLab training material is provided after the training concludes. GitLab training material is provided for internal use only.

| |
|---|
| Education - GitLab CI/CD Training *Provide private Instructor-led GitLab CI/CD Training.* |
| **Included**<br>• Provide training for the following focus areas:<br>○ Describe what CI/CD is. ○ Explain how runners work. ○ Set up and configure CI/CD and runners. |
| ○ Verify a new feature.<br>○ Scope and persist variables at various levels. ○ Scaffold out the basics of a test, build, review, and deploy pipeline, leveraging feature/topic branching as the review mechanism.<br>○ Release and deployment workflow. ○ Artifacts and dependency caching. ○ Building and deploying images to GitLab registry. |
| **Assumptions**<br>• Attendees will have access to Gitlab accounts with Configured runners.<br>• Attendees must confirm with the training coordinator that all system requirements (https://university.gitlab.com/pages/gitlab-ilt-sysreq/) for the class have been met prior to the class start date.<br>• Attendees must have access to web browsers other than Internet Explorer.<br>• Attendees will participate in practice exercises (labs).<br>• Remote ILT class(es) is delivered in a single day, including a 1-hour break for lunch.<br>• Remote ILT class(es) may finish early depending on attendee feedback and lab participation.<br>• Attendees are required to join web conference sessions with cameras enabled to foster interactive sessions.<br>• Recording and/or distribution of recordings of ILT classes in any way is strictly prohibited unless explicitly provided by GitLab in writing prior to such recording or distribution.<br>• Training accommodates 12 participants, with a maximum capacity of 15 participants available through the purchase of 3 additional seats. |

**Deliverables**

GitLab training material is provided after the training concludes. GitLab training material is provided for internal use only.

Education - GitLab Security Essentials Training *Provide private Instructor-led GitLab Security Essentials Training.*

**Included**

- Describe the security features available in GitLab.
- Determine teams and/or team members that should give merge request security approvals.
- Enable and configure scanning tool, including enabling and disabling options.
- Enable and configure merge request security approvals.

- View and utilize the Security Dashboard for a given group and project.
- Download scanning results as evidence for compliance.
- Configure defensive mechanisms.
- Test performance and inspect logs.
- More details relating to the course can be found at https://about.gitlab.com/services/education/security-essentials/

**Assumptions**

- Attendees will have access to Gitlab accounts with Configured runners.
- Attendees must confirm with the training coordinator that all system requirements (https://university.gitlab.com/pages/gitlab-ilt-sysreq/) for the class have been met prior to the class start date.
- Attendees must have access to web browsers other than Internet Explorer.
- Attendees will participate in practice exercises (labs).
- Remote ILT class(es) is delivered in a single day, including a 1-hour break for lunch.
- Remote ILT class(es) may finish early depending on attendee feedback and lab participation.
- Attendees are required to join web conference sessions with cameras enabled to foster interactive sessions.
- Recording and/or distribution of recordings of ILT classes in any way is strictly prohibited unless explicitly provided by GitLab in writing prior to such recording or distribution.
- Training accommodates 12 participants, with a maximum capacity of 15 participants available through the purchase of 3 additional seats.

**Deliverables**

- GitLab training material is provided after the training concludes. GitLab training material is provided for internal use only.

Education - GitLab Duo Enterprise Training

*Provide training related to the effective integration of GitLab Duo integration in your development processes.*

**Included**

- Provide training for the following focus areas: ○ Intro to AI at GitLab ○ Getting Started with GitLab Duo ○ Use of Duo in Issues and Merge Requests ○ GitLab Duo Code Suggestions ○ Resolving Vulnerabilities with Duo ○ GitLab Duo Chat

**Assumptions**

- Attendees will have access to Gitlab accounts with Configured runners.
- Attendees must confirm with the training coordinator that all system requirements (https://university.gitlab.com/pages/gitlab-ilt-sysreq/) for the class have been met prior to the class start date.
- Attendees must have access to web browsers other than Internet Explorer.
- Attendees will participate in practice exercises (labs).
- Remote ILT class(es) is delivered in a single day, including a 1-hour break for lunch.
- Remote ILT class(es) may finish early depending on attendee feedback and lab participation.
- Attendees are required to join web conference sessions with cameras enabled to foster interactive sessions.
- Recording and/or distribution of recordings of ILT classes in any way is strictly prohibited unless explicitly provided by GitLab in writing prior to such recording or distribution.
- Training accommodates 12 participants, with a maximum capacity of 15 participants available through the purchase of 3 additional seats.

**Deliverables**

- GitLab training material is provided after the training concludes. GitLab training material is provided for internal use only.

| Education - GitLab Certifications Exams<br>*Provide Certification redemption codes to redeem for 1 attempt each at GitLab technical certifications.* |
|---|
| **Included**<br>• Provide certification redemption codes that can be used to undertake a GitLab Technical Certification. The Certifications available are:<br>o GitLab Certified Git Associate o GitLab Certified CI/CD Associate<br>o GitLab Certified Project Management Associate<br>o GitLab Certified Security Specialist o GitLab Certified DevOps Professionals |
| **Assumptions**<br>• Trainees will complete either self-paced training or attend an instructor-led training course prior to testing for certification.<br>• Instructor-led training is not included with the certification exam codes.<br>• Exam codes are valid for 12 months from the date of purchase. |
| **Deliverables**<br>• Redemption codes |

**APPENDIX B - STANDARD WORK AUTHORISATION**

| Standard Work Authorisation Request | | | | |
|---|---|---|---|---|
| Customer Group Name | | | | |
| Activity | Tentative Start Date | Tentative End Date | Number of Days | Total Fee |
| | | | | |
| | | | | |
| | | | | Total Fee |
| | | | | |
| Approver Name | Approval Date | | | |
| | | | | |
| Acceptance | | | | |

**APPENDIX C - DESCRIPTION OF WORK TEMPLATE**

# Description of Work

| | |
|---|---|
| Effective Date | |
| Version | |

| | |
|---|---|
| DOW # | |
| Customer Group Name | |
| Customer Group Contact | |
| GitLab Contact | |
| GitLab Utilization of Subcontractor (if applicable) | If a partner is utilized for subcontracting services please see the applicable list of subcontractors / subprocessors here: https://about.gitlab.com/privacy/subprocessors/#professional-servicessub-processors<br>If the supplier advises the requirement is to be fulfilled via a subcontracted party, then depending on the engagement route and IR35 status, confirmation will be required on the requirement to issue a Status Determination Statement before engagement commences. |

# DESCRIPTION AND AUTHORIZATION

## Executive Summary

<HIGH LEVEL DESCRIPTION OF BUSINESS OBJECTIVES> Effort estimates provided here are for example and are based on the GitLab approach, key metrics, mutual obligations and assumptions. A material change, exception to approach or an unanticipated circumstance (e.g. environment issues, lack of resource availability, etc.) may require a change in scope and therefore a deviation from our standard effort.

# PROFESSIONAL SERVICES DESCRIPTION

In performance of the Professional Services herein, GitLab will perform the project activities as defined in;

<DESCRIPTION OF PROFESSIONAL SERVICES ACTIVITIES>

Effort estimates provided here are for example and are based on the GitLab approach, key metrics, mutual obligations and assumptions. A material change, exception to approach or an unanticipated circumstance (e.g. environment issues, lack of resource availability, etc.) may require a change in scope and therefore a deviation from our standard effort.

# PROJECT ASSUMPTIONS

## Scheduling & Work Structure

When executing project activities;

1. Service Delivery:

a. All work will be performed remotely (no travel authorized) unless mutually agreed upon
b. Standard hours are 9am-5pm Monday-Friday in mutually agreed-upon time zone
c. Non-standard hours require 10 business days advance notice and mutual agreement
d. Work will run contiguously unless explicitly stated otherwise 2. GitLab Team Availability:
a. Delivery teams follow official government holidays of service delivery location
b. Minimum weekly commitment of 40 hours of work required
c. Project ceremonies must include full working team or delegates with decision authority

3. Schedule Changes & Delays:

a. Delays over five business days due to Customer Group readiness may result in suspended delivery, in which case Customer Group shall bear the additional cost of restarting the project
b. Schedule modifications based on changes in understood scope as laid out in this document after the delivery of the project plan will require a Change Order and may incur additional fees
c. The Customer Group must provide 10 days' notice for rescheduling/cancellation of project kickoff date

4. Mobilisation

a. After identification of need, selection of Activity and approval from the ECS Governance team, a Standard mobilisation time of 4 working weeks applies. Mobilisation times can be improved with forward planning and regular engagement between GitLab Engagement Manager/ Program Manager and ECS Governance team.

## Technical & Project Scope

1. Technical Constraints:

a. Solutions based on GitLab version features available at contract execution date

b. Project management will use a mutually agreed platform for collaboration and storing project artefacts.
c. GitLab will work with Customer Group to identify appropriate web conference tooling for all ceremonies

i.Customer Group responsible for ensuring appropriate distribution to their resources

d. There are two migration approaches for Dedicated, GEO and Congregate, these are the initial decision points.

| **Decision Factor** | **GEO Migration** | **Congregate Migration** |
|---|---|---|
| Source Platform Compatibility | Only GitLab Self Managed | Supports all platforms (GitLab.com, GitHub.com, GitHub enterprise Bitbucket server, Bitbucket cloud, GitLab Self-Managed, Azure DevOps Repos) |
| Connectivity | Network connectivity to a Customer Group-managed database replica | Ability to install VM in Customer Group networks / premises with network connection to source and destination systems |
| Job Artifact Migration | Supported | Not Supported |

2. Access Requirements:
a. The Customer Group must provide system administrator access where needed
b. The Customer Group responsible for acquiring/managing all third-party product licenses
c. The Customer Group must handle internal software installation and usage approvals

## Customer Group Responsibilities

1. Senior Customer Group Stakeholder

a. ECS ALM are identified as overall Dedicated GitLab Platform Owner
b. Each Customer Group will have a sub Platform/Product Owner

c. Responsible for Customer Group representation within program steering committee
d. Will attend and support the activities for regular steering committee meetings
e. Acts as Senior escalation point for GitLab
f. Leads initial introductions for GitLab team into Customer Groups.

2. Customer Group Project Management:

a. Responsible for Customer Group program and resource management
b. Manage the engagement and availability of personnel with appropriate skills, access, and decision-making authority
c. Must provide and maintain access to accurate technical documentation in regard to the Customer Group's environments, processes, and requirements.
d. Drives Customer Group readiness and resolution of blockers to maintain the ongoing delivery velocity of the project.
e. Responsible for coordinating maintenance windows required to transition.

3. Resource Availability:

a. GitLab will provide 10 working days notice in advance to Customer Group when requesting skilled resources.
b. Must provide direct contact with key personnel (program lead, users, admins, dev/ops teams)
c. Must provide subject matter experts for technical discussions

i. The Customer Group's failure to meet obligations impacts GitLab's ability to perform services as estimated in this agreement. Delays resulting from Customer Group readiness will trigger a change management process that will incur additional cost.

4. Customer Group Technical Responsibilities

a. Depending on the migration type, the Customer Group will need to provide access to a replica database instance for GEO migration or for congregate migrations they will need to provide a VM in their network from which we will carry out the migration.

5. Onboarding Support

a. Customer Group responsible for providing clear guidance for onboarding to the Customer Group environment, including Laptop provisioning, VPN access, System entitlements, and any required training. Extended Onboarding Activities will need to be mutually agreed upon and may draw down from total T&M hours.
b. Where Security Clearance is necessary, the Customer Group team will work with GitLab Professional Services to enable suitable candidates with Security Clearance requirements. The Customer Group team will provide a list of suitability requirements.

Joint Activity Management Responsibilities and Tasks

1. Both GitLab and Customer Group Project Leads will ensure the following responsibilities and tasks are met as are reasonably applicable to the Professional Services being performed.
2. Coordinate, schedule and monitor all resources and activities related to the Professional Services described in this DOW.

3. Coordinate and monitor all project change process activities related to the Professional Services described in this DOW.
4. Act as the focal points for communications between GitLab and Customer Group during the provision of all Professional Services described in this DOW.
5. Attend Customer Group and GitLab status meetings, as applicable.
6. Upon becoming aware of a situation which may delay, or threatens to delay, the timely performance of this DOW, promptly communicate this information to the Project Manager who is not aware.

# SCHEDULE AND EFFORT ALLOWANCES

Activities outlined in this Description of Work are scheduled to commence two calendar weeks not to exceed six weeks post DOW execution with a mobilisation meeting in which the parties will review the outlined scope, dependencies, and resources requirements and establish a refinement and roadmap build for the Professional Services engagement cadence. Subsequent to the mobilisation meeting a schedule of activities will outline the most effective and efficient approach to complete the estimated scope.

In the event Customer Group needs to reschedule or cancel the Professional Services engagement, Customer Group shall provide GitLab with ten (10) business days' prior written notice (email shall suffice). If Customer Group fails to provide such notice, Customer Group shall pay GitLab's costs directly associated with rescheduling the engagement.

## Effort Allowances

Customer Group acknowledges that they may need to request additional Professional Services if the migration to Dedicated Platform is unable to be completed within the effort allowance. Any additional Professional Services or scope changes will be documented in the form of a new DOW or Change Order requested by the parties' authorized representatives and approved by ECS before GitLab will proceed.

| | **Quantity** |
|---|---|
| Effort Allowance | |

1. In performance of the Professional Services described, GitLab shall perform the project activities listed in this DOW utilising the pre-billed fixed fee amounts detailed in the Effort Allowances.
2. GitLab will:

a. Provide monthly budget utilization reports aligned with the project plan
b. Alert Customer Group promptly of any potential budget risks
c. Not exceed the estimated days without Customer Group's written approval
d. Not commence a new work activity without an approved Work Authorisation from ECS Governance team

3. Additional time and fees may be required if:

a. Material changes occur to project scope or complexity after plan acceptance
b. Key assumptions or requirements are not met
c. Any changes requiring additional days must be approved via Change Order before work begins.

4. Travel & Expense

a. All reasonable travel expenses incurred by GitLab personnel in performance of the Services under this DOW shall be reimbursed by Customer Group at cost, including but not limited to airfare, ground transportation, lodging, and meals. Travel expenses require Customer Group's prior written approval for any trip with all reasonable costings outlined ahead of time for approval by the Customer Group. All expenses must be supported by original receipts and submitted within [30] days of incurrence.

b. The GitLab Professional Services team will deliver services subject to any reasonable travel and expense policy provided by Customer Group prior to project kickoff. If the travel and expense policy is not provided in a timely manner, or the Customer Group does not have a travel policy for contractors, then the GitLab Professional Services team will deliver services subject to GitLab's own internal travel and expense policies.

## Changes to Scope

Will require;

1. Written identification from GitLab or written request from Customer Group
2. GitLab estimate of time and cost to complete
3. Mutual agreement via Change Order

# Requesting, Approval and Scheduling Activities

1. ECS Governance team will make requests to either GitLab scoping representative (Engagement Manager or GitLab Program/Project Manager) to engage with a Customer Group.
2. GitLab scoping representative will engage in a discovery with Customer Group and identify their Activity needs.
3. GitLab scoping representative will validate and provide back to Customer Group an Activity requirement in the form of a Work Authorisation document (see Appendix B).
4. Customer Group will either iterate with GitLab scoping representative or pass Work Authorisation directly to ECS Governance team for approval.
5. ECS Governance team will approve/iterate/decline Work Authorisation request.
6. Once approved, ECS Governance team will advise GitLab scoping representative who will then send approved Work Authorisation to GitLab delivery team for team mobilisation and activity execution.

Note: A Work Authorisation is only deemed as approved for mobilisation and execution when fully executed by both GitLab and ECS signatories.

Note: Work Authorisations can be approved but may not be scheduled if the remaining budget is not sufficient to cover the days required to execute.

## Acceptance of Fixed Fee Services (Education)

**Training**: To the extent Customer Group has purchased training, acceptance will be deemed to have occurred upon GitLab's confirmation of the list of attendees.

**Technical Certification redemption codes**: To the extent Customer Group has purchased. Certification redemption codes, acceptance will be deemed to have occurred upon GitLab's delivery of redemption codes via email.

Throughout the project, GitLab will collaborate with Customer Group through agile ceremonies, through which work will be prioritized, delivered and reviewed on a continuous basis. As such, once the final Activity completes, the project is considered complete and delivered.

# AUTHORIZATION

The parties hereto, duly represented by an authorized signatory, for and behalf of the business entity it represents, hereby agree to be bound by the terms set forth in this DOW and the Contract between the parties, including the Professional Services Annex to Special Terms 1, which are fully incorporated by reference herein. For purpose of clarity, the terms of this DOW shall supersede any prior agreement(s) between the parties.This DOW may be withdrawn by GitLab if not executed by Customer on or before <DATE>

| GitLab UK Ltd | <CONSUMER_GROUP> |
|---|---|
| Company name | Company name |
| | |
| Full name | Full name |
| Title | Title |
| Signature | Signature |
| Date | Date |