exponential-e
APPLIED INNOVATION

UK MANAGED SERVICES

RM1557.15 G-Cloud 15 Supplier Terms

HM Government G-Cloud

Crown Commercial Service *Supplier*

bsi. ISO 9001 Quality Management | ISO 27001 Information Security Management | ISO/IEC 20000-1 Information Technology Service Management | CSA STAR Cloud Security | ISO 22301 Business Continuity Management | ISO 50001 Energy Management | ISO 14001 Environmental Management | BS 10012 Data Protection | ISO 27017 Security Controls for Cloud Services

CCS Approved Supplier:

RM1557.15 G-Cloud 15, RM3764.3 Cyber Security Services 3 DPS, RM6116 Network Services 3, RM6190 Technology Services 4, RM1043.9 Digital Outcomes (DOS) v7, RM3825 HSCN DPS, RM6094 SPARK DPS; RM6200 Artificial Intelligence DPS

PCI | CYBER ESSENTIALS CERTIFIED PLUS | HSCN

Table of Contents

UK Managed Services Supplier Terms

Section 1: Acceptable Use Policy

Not Used

Section 2: DPA

This Data Processing Addendum ("DPA") applies between the Supplier ("Data Processor") and the Buyer hereinafter referred to as “the Buyer” and/or "Data Controller", collectively referred to as the "Parties" and individually as a "Party".

Under this DPA, the Data Processor agrees to process personal data received from the Data Controller solely on behalf of the Data Controller and in compliance with (i) the instructions received from the Data Controller; (ii) the General Data Protection Regulation (GDPR); and (iii) the Data Protection Act 2018.

Any terms capitalized but not defined herein shall have the meaning ascribed to them in the Principal Agreement or applicable legislation. This DPA is subject to the terms and conditions set forth in the Principal Agreement, except where explicitly modified by this DPA.

1. DEFINITIONS

1.1 For the purposes of this DPA, the following terms shall have the meanings set forth below:

“Buyer Data”	**Personal Data of Data Subjects which the Buyer is either the Controller or Processor of;**
“Data Processor”	Supplier, in its role of processing personal data on behalf of the Data Controller;
“Data Controller”	The Buyer, in its role of determining the purposes and means of the processing of personal data;
“Data Protection Laws”	(i) the Data Protection Act 2018 (and any re-enactment or replacement thereof), (ii) the GDPR; (iii) the UK GDPR and (iv) any other applicable statutes and regulations regarding the Processing of Personal Data;
“Data Subject”	an identified or identifiable natural person;
“GDPR”	The General Data Protection Regulation (Regulation (EU) 2016/679)
“Principal Agreement”	The GCloud Call Off Contract between the Data Processor and Data Controller for the purchase of services;
“Personal Data”	Any information relating to an identified or identifiable natural person that is processed under this DPA. For the avoidance of doubt, 'Personal Data' shall be interpreted in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the UK General Data Protection Regulation ("UK GDPR");
“Processing”	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as 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. 'Processing' shall also be interpreted in accordance with the GDPR and UK GDPR.

2. Scope and Roles

2.1 This DPA applies when Buyer Data is processed by Supplier. For the purpose of this DPA, Supplier (as applicable) will act as a Data Processor, and the Buyer will act as a Data Controller, who may act itself as either a Controller or Processor of Personal Data. Service specific processing (where applicable) will be detailed in the Appendix to this DPA.

2.2 Both parties agree to comply with their respective obligations under the Data Protection Laws. The Data Processor agrees to process Personal Data only on documented instructions from the Data Controller, unless required by the laws of England and Wales or any other relevant country to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.3 Supplier shall maintain complete and accurate records of its Processing activities under the relevant Call-Off Contract in accordance with the Data Protection Laws and make such records available for inspection by the Buyer as soon as reasonably practicable following written request by the Buyer.

3. Buyer instructions

3.1 The Parties agree that this DPA and the Principal Agreement constitute the documented instructions provided herein. These instructions are to Process Personal Data:

(a) exclusively for the purposes set forth in the Principal Agreement, and not for any other purpose unless expressly authorised in writing by the Data Controller; and
(b) only to the extent reasonably necessary to provide the relevant Service(s) and exercise its rights and fulfil its obligations under, and in accordance with, the Call-Off Contract; and
(c) in compliance with the Data Protection Laws.

3.2 Taking into account the nature of Services and Processing, the Buyer acknowledges that it is unlikely that Supplier will be able to know whether an instruction infringes the Data Protection Laws. In the event that Supplier is of the opinion that such instructions may infringe the Data Protection Laws, it shall immediately inform the Data Controller.

3.3 Any such additional instructions outside of the scope of this DPA and the Principal Agreement require the prior written agreement of Supplier and may result in additional fees being payable by the Buyer.

3.4 The Buyer is entitled to terminate this DPA and the Principal Agreement (subject to the payment of the Termination Payment) in the event that Supplier declines to follow any instructions requested by the Buyer outside of the scope of this DPA and Principal Agreement.

3.5 Supplier shall follow any such instructions in this DPA and Principal Agreement unless applicable law requires otherwise; in such cases, Supplier shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4. Confidentiality of Buyer Data

4.1 Supplier will not access, use or disclose to any third party, any Buyer Data save where (i) necessary to maintain or provide Services; and/or (ii) to comply with the law or a valid and binding order of a governmental or investigatory body. Where required to comply with a governmental or investigatory body, Supplier may information to the minimum extent required to comply with any such order.

4.2 Supplier shall promptly notify the Buyer of any request received directly from a Data Subject.

4.3 All employees, agents, or subcontractors of Supplier who have access to Personal Data under this DPA are required to maintain the confidentiality of such information and are prohibited from using the information for any unauthorized purpose.

5. Security of Data Processing

5.1 In accordance with the DPA, Supplier shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes associated with the processing of Personal Data. Subject to any service-specific details set out in an Appendix to this DPA, such measures shall include, but may not be limited to, the following:

(d) Maintaining relevant accreditations, including ISO27001 and CSA STAR (where applicable to the Service in question) or any materially-equivalent or replacement standards, to demonstrate compliance with industry standards for information security management;

(e) Ensuring that access to Personal Data is limited to authorized personnel who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(f) Regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

(g) Implementing industry-standard measures to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(h) Ensuring that all processing activities are conducted in compliance with the Data Protection Laws.

6. Assistance

6.1 Supplier will assist upon request the Data Controller in responding to any request from a Data Subject and in ensuring compliance with its obligations under the GDPR and UK GDPR with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators. Any such assistance shall be provided at Supplier's then current standard rates for Professional Services.

7. Sub-Processing

7.1 The Buyer provides authorisation for Supplier's use of the sub-processors set out in the appendix to this DPA ("Sub-processors").

8. Data Breach Notification

8.1 In the event of a Personal Data Breach, Supplier shall notify the Data Controller without undue delay, and in any event within seventy-two (72) hours after having become aware of it. This notification may be provided in phases where all information it is not possible to provide all information at the same time.

9. Data Transfer

9.1 In accordance with the DPA and the Data Protection Laws, the Data Processor and Data Controller acknowledge that the Data Processor may transfer Personal Data outside of the European Economic Area (EEA) and/or United Kingdom, subject to Paragraph 9.2 below

9.2 Supplier shall ensure that any such transfer of Personal Data is subject to appropriate safeguards as may be required by the GDPR and UK GDPR, including the execution of Standard Call-Off Contractual Clauses approved by the European Commission or relying on an adequacy decision by the European Commission, where applicable.

9.3 In the event of any conflict between the provisions of this Data Transfer clause and any other provisions of the DPA or the Principal Agreement, the provisions of this Data Transfer clause shall prevail with respect to the transfers of Personal Data.

10. Audit

10.1 Subject to the remaining provisions of this Paragraph 10.1, the Buyer may, at a mutually agreed time, conduct an audit to verify Supplier's compliance with its Processing obligations under this DPA. Supplier and the Buyer shall use all

reasonable endeavours to schedule the audit within one (1) calendar month of request.

10.1.1 Subject to the remaining provisions of this Paragraph 10.1, Supplier shall provide the Buyer with all reasonable assistance to carry out the audit, including access to relevant premises, systems, records and personnel. Access to records and systems shall be strictly limited to those areas solely containing data relating to the Processing of Buyer Personal Data under the Principal Agreement. No access to (i) data pertaining to other Buyers and/or (ii) any other information that is covered by a confidentiality obligation to a third party and/or (iii) any financial or commercially-sensitive information pertaining to the Buyer will be provided.

10.1.2 Any audit shall be carried out during Normal Business Hours and no more frequently than once in any twelve (12) month period unless stipulated otherwise by the Data Protection Laws.

10.1.3 The Buyer shall (and shall procure that all auditing personnel shall) comply with the reasonable (i) site security and health and safety policies and procedures applicable to Supplier's premises and (ii) instructions of any supervising Supplier personnel, whilst carrying out the audit.

10.1.4 The Buyer shall (and shall procure that all auditing personnel shall) ensure that the audit is carried out in such as manner so as not to unreasonably disrupt the normal business operations of Supplier and is carried out in an expeditious and professional manner by suitably qualified personnel.

10.1.5 Supplier reserves the right, at all times, to refuse entry to its premises and/or systems, and/ or records or to remove from its premises to, and/or remove system and/or records access rights for, any person who in the reasonable opinion of Supplier is not fit to have such access or is causing the Buyer to be in breach of this Clause 10.1.

10.1.6 Supplier shall be entitled to charge for its time incurred as a result of any audit under this Paragraph 10.1 at a rate of £2,000 ex VAT for each Working Day or part thereof, save where such audit finds that Supplier has failed to comply with its Personal Data Processing obligations under this DPA.

11. Term and Termination

11.1 This DPA shall commence upon entering into the Principal Agreement and shall remain in effect until the termination or expiry of the Principal Agreement, unless otherwise terminated in accordance with its terms. Upon termination of the Principal Agreement, this DPA shall automatically terminate without the requirement of further notice.

11.2 Upon termination of this DPA for any reason, Supplier and the Buyer shall comply with any Return of Personal Data section of the Appendix to this DPA (if applicable). Where the Personal Data has not been removed pursuant to the Appendix, Supplier shall be entitled to delete the same without further liability to the Buyer (unless local laws (for the purpose of processing within the UK) or European Union or Member State law (where processing occurs in within the EEA) requires the continued storage of the Personal Data).

11.3 The obligations of confidentiality and data protection set forth in this DPA shall survive the termination of this DPA for a period of five (5) years.

Appendix to the DPA

Subject Matter of Processing

The Personal Data (if any) that the Buyer stores within the applications managed by the Supplier and the Buyer's Active Directory.

Nature of the Processing

As reasonably required to provide the UK Based Managed Service.

Supplier will not block, delete, correct, pseudonymise or encrypt any data. Supplier has no responsibility for data accuracy in respect of the Buyer data.

Section 3: Supplier Specific Shared Responsibility Model

3.1 The Buyer shall comply with any Buyer responsibilities set out in any Shared Responsibility Model applicable to the Call-off Contract in a timely manner.

3.2 Any delay or failure of the Buyer in performing its obligations under Clause 3.1 above, shall relieve the Supplier of performing any impacted obligations/fulfilling any impacted responsibilities that it has under the Call-off Contract.

Section 4: Service Levels

4.1 Service Levels are targets which the Supplier will use all reasonable endeavours to achieve but which are not guaranteed.

4.2 Unless set out specifically otherwise in the applicable Call-Off Contract, service credits (where available) are the sole remedy for any failure to meet Service Levels.

4.3 Service credit claims must be submitted to clientrelations@exponential-e.com within one (1) month of the end of the calendar month in which the failure to meet the target service level occurred. Any service credit claims not raised by the Buyer within this period are irrevocably waived.

4.4 If service credits are rightly due, they shall be calculated in accordance with the Call-off Contract (such service credits being a genuine pre-estimate of loss, not a penalty and not unconscionable) and shall be applied to the Buyer's account.

Section 5: Licence Terms for Cloud Products

Not Applicable