exponential-e
APPLIED INNOVATION

UK BASED FLEXIBLE SUPPORT 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

Flex Support Service Supplier Terms

Section 1: Acceptable Use Policy

1.1 The Buyer shall comply (and shall procure that all users of the Services comply) with the following. It is prohibited for any user to participate in any of the activities listed below (whether actual or attempted and whether directly or indirectly) in relation to Supplier's Services:

- Other than for legitimate business reasons, posting or sending messages substantially similar in content to 10 or more Usenet or other newsgroups, forums, listservs, or other similar groups or lists (each, a "List");
- Other than for legitimate business reasons, posting or sending messages, articles, or other content to a List which are off-topic according to the charter or other owner-published FAQs or descriptions of the List;
- Sending unsolicited commercial messages or communications in any form such as unsolicited bulk emails or text messages, 'mailbombs', nuisance calls or advertising ("SPAM");
- Falsifying user or other Service-related information, including, but not limited to, intentionally omitting, deleting, forging or misrepresenting transmission information, including headers, return mailing and Internet protocol addresses, provided to Supplier or to other service users or engaging in any activities or actions intended to withhold or cloak Buyer's or a user's identity or contact information;
- Engaging in any activity that:
    - threatens the integrity and/or security of any network or computer system (including, but not limited to, transmission of worms, viruses and other malicious codes and accessing any device or data without proper authorisation);
    - attempts to use the Service in such a manner so as to avoid incurring charges for or otherwise being required to pay for such usage;
    - violates generally-accepted standards of Internet or other networks conduct and usage, including, but not limited to, denial of service attacks, web page defacement, port and network scanning, and unauthorised system penetrations, probes, scans and/or tests;

- prevents, blocks or obstructs access to any programme installed on, or data saved in, any computer or damage or harm the operation of any of these programmes or the reliability or accuracy of any of this data;
- promotes or encourages socially-unacceptable or irresponsible behaviour, or that may be otherwise harmful to any person or animal;
- breaches privacy and/or data protection and/or intellectual property rights;
- misrepresents or impersonates another person, or help others to do the same, which includes faking, forging or hiding email headers, subjects, sender details or caller ID details;
- In Supplier's reasonable opinion causes annoyance, inconvenience, distress, offence or anxiety to any person;
- In Supplier's reasonable opinion could be considered offensive on the grounds of race, sex, religion, nationality, disability, sexual orientation, age or any other similar categorisation;
- In Supplier's reasonable opinion is fraudulent and/or dishonest;
- In Supplier's reasonable opinion is detrimental to other users of the internet and/or other Supplier Buyers.

- Using Supplier's services to guess passwords or access systems or networks without written authorisation;
- Engaging in any of the activities listed above by using another provider's service, but channelling the activity through a Service Provider account, remailer, or otherwise through a Service;
- Configuring Buyer systems to bypass security controls, including the installation of programs or services that allow the systems to be managed or accessed insecurely or through unauthorised means;
- Conducting online security audits or tests against or through Supplier systems or networks without coordination with and the explicit, written consent of an authorized officer of Supplier;
- Gaining, or attempting to gain, unauthorised access to Supplier networking, security, management, backup, storage or monitoring systems;
- Installing programs or configuring systems to allow the monitoring, or "sniffing," of data traveling over a shared network;

- Accessing, or attempting to access, security-relevant information, such as password files that may, among other things, be used to gain unauthorised access to system accounts;
- Installing or using software for the purpose of cracking encrypted data, including stored passwords;
- Removing or disabling security software or services, including anti-virus software, logging utilities or authentication services;
- Transferring Remote-access accounts from one individual to another or sharing, or permitting the sharing of, the same. Individual remote-access accounts that uniquely and accurately identify the owner of the account shall be maintained as such by the Buyer;
- In contravention of any relevant Ofcom regulations including relating to nuisance calls;
- Attempting to gain access to any electronic systems, networks or data, without proper consent;
- Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP;
- Making an unwanted or hoax call that causes annoyance to the receiver of the call, and/or is of an offensive, spiteful, abusive, indecent, defamatory, obscene or menacing nature including unauthorised or ‘spam’ Calls and ‘silent’ Calls as defined by Ofcom in its ‘Statement of policy on the persistent misuse of an electronic communications service’ published 1 March 2006, and any subsequent update;
- using the Service in any way that violates applicable law and/or regulations, or acting or omitting to act in any way which will place Supplier in breach of applicable laws and/or regulations including but not limited to the Communications Act 2003;
- using the Service in any way that would constitute or contribute to the commission of a crime, tort, fraud or other unlawful activity (including activities deemed unlawful under a complainant’s jurisdiction);
- allowing any unauthorised user or third-party access to, or use of Services and shall take all reasonable security measures to prevent the same;
- adding to, modifying or interfering in any way with the Service(s);

1.2 The Buyer shall (at its cost):

- comply with all reasonable codes of practice, procedures and directions as are established or adopted by Supplier in relation to Numbers; and
- ensure that any equipment not forming part of the Services and which is connected (directly or indirectly) to the Services will be technically compatible and interoperable with the Services and approved for that purpose under any applicable laws and it will not interfere with the operation of the Services; and
- provide (and shall procure that any relevant third-party vendor/supporter provides) such reasonable assistance as Supplier shall require in relation to any agreed inter-operability of the Supplier Services with any equipment not forming part of the Services and which is connected (directly or indirectly) to the Services;
- obtain effective and keep effective all permissions licences and permits which may from time to time be required in connection with the use of any Supplier equipment provided as part of the Services and to comply with all statutory and other obligations in relation to the use of the such Supplier equipment; and
- keep the Supplier equipment at the Buyer's sites; and
- return any faulty Supplier equipment to Supplier as soon as reasonably possible, but in any event within ten (10) Working Days. Should the faulty unit not be returned as required, Supplier shall have the right to charge the full current retail price for a replacement item; and
- comply with any applicable portal terms of use;

1.3 The Buyer warrants that any material and/or communication received, transmitted, hosted or otherwise processed using the Services (other than entirely unsolicited communications) will not be menacing, of a junk-mail or spam-like nature, illegal, obscene, threatening, defamatory, discriminatory, promote illegal or unlawful activity, be otherwise actionable or in violation of applicable laws and/or regulations to which the use of the Service(s) is subject.

1.4 The Buyer is responsible for (and shall be liable to Supplier in respect of):

- the use of the Service(s) (including any incurred charges) by any of its employees and any other person who has been given access to the Service(s) by the Buyer or who has obtained access to the Services which is not due to Supplier's breach of the Call-Off Contract and/or negligence even if such use was not authorised by the Buyer;
- the safety, safe custody and safe use of Supplier equipment whilst it is in the Buyer's custody and the Buyer shall be liable to Supplier for any loss or damage to the Supplier equipment except for (i) fair wear and tear and (ii) any

loss or damage caused by the negligent act or omission of Supplier, its employees, Call-Off Contractors or agents.

1.5 In the event that the Buyer is provided with access to a third-party licence by Supplier, the Buyer agrees to abide by any third-party software conditions of use as set out in any relevant End User License Agreements (EULA) provided or made available to the Buyer by Supplier (whether via the portal or otherwise). The Buyer shall (and shall procure that all users of the Software shall) only use the Software in accordance with such EULA.

1.6 Supplier may suspend provision of the Service(s) in the event of:

(i) suspected fraudulent call activity in accordance with its Fraudulent Calls Process (as current from time to time) (copy available upon request from sales@exponential-e.com; and/or

(ii) material breach of this AUP.

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:

(a) 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;

(b) 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;

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

(d) 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

(e) 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

Not Applicable

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