

# The contract variation for G-Cloud 9

The Crown Commercial Service (CCS) has made some minor changes to the framework agreement and call-off contract (reference RM1557ix) because of the new General Data Protection Regulation (GDPR).

## Framework agreement

### Clause

8.57	<p>a) The provisions of these Data protection and disclosure clauses 8.57 to 8.62 (inclusive) will apply during the Term and for as long as the Supplier holds CCS Personal Data.</p> <p>b) The Parties will comply with the Data Protection Legislation for the purposes of which CCS is the Controller and the Supplier the Processor. The only processing the Supplier is authorised to do (unless otherwise required by Law) in respect of its contractual relationship with CCS under this Framework Agreement is:</p> <ul style="list-style-type: none"><li>• restricted to operations that are strictly necessary for the management/administration of this Framework Agreement; and</li><li>• is limited to Personal Data relating to CCS and Buyer personnel, such as contact details, strictly required for the fulfilment of the Supplier's obligation under this Framework Agreement.</li></ul>
------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

8.58	<p>a) The Supplier must comply with any notification requirements under the <del>Data Protection Act (DPA)</del> Data Protection Legislation and both Parties will observe their obligations under it.</p> <p>b) The Supplier will notify CCS immediately if it receives any communication from a third party relating to the Parties' obligations under the Data Protection Legislation, or becomes aware of a Data Loss Event and will provide CCS with full and ongoing assistance in relation to each Party's obligations under the Data Protection Legislation in accordance with any timescales reasonably required by CCS.</p> <p>c) The Supplier will provide all reasonable assistance to CCS to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to processing operations, risks and measures) and must notify CCS immediately if it considers that CCS's instructions infringe the Data Protection Legislation.</p>
8.59	<p><del>If the Supplier is processing CCS's or Buyers' Personal Data, the Supplier must have appropriate technical and organisational processes to ensure its security. The Supplier must guard against unauthorised or unlawful processing, loss or destruction of the Personal Data.</del></p> <p>a) The Supplier must have in place Protective Measures to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.</p> <p>b) The Supplier will ensure that the Supplier Staff only process Personal Data in accordance with this Framework Agreement and take all reasonable steps to ensure the reliability and integrity of Supplier Staff with access to Personal Data.</p> <p>c) CCS may amend this Framework Agreement on not less than 30 Working Days' notice to the Supplier to ensure that it complies with any guidance issued by the Information Commissioner's Office.</p>

8.60

The Supplier will:

- provide CCS and the Buyer with any information they may reasonably request to ensure the Supplier is complying with all of its obligations under the Data Protection Legislation which arise in connection with the Framework Agreement or under a Call-Off Contract
- ~~• promptly tell CCS and the Buyer about any breach of this data protection clause~~
- ensure that it doesn't knowingly or negligently do or omit to do anything which places CCS or Buyers in breach of their Data Protection Legislation obligations
- ~~• not cause or permit to be processed, stored, accessed or otherwise transferred outside the European Economic Area any CCS or Buyer Personal Data without written approval~~
- not transfer Personal Data outside of the European Economic Area unless the prior written consent of CCS has been obtained, and
  - i. CCS or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by CCS;
  - ii. the Data Subject has enforceable rights and effective legal remedies;
  - iii. the Supplier 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 CCS in meeting its obligations); and
  - iv. the Supplier complies with any reasonable instructions notified to it in advance by CCS with respect to the processing of the Personal Data;
- before allowing any Subprocessor to process any Personal Data related to this Framework Agreement, obtain the prior written consent of CCS and shall remain fully liable for the acts and omissions of any Subprocessor
- maintain complete and accurate records and information to demonstrate its compliance with clauses 8.57 to 8.62

Schedule 3 - Glossary and interpretations	<p><b>Controller</b></p> <p>Takes the meaning given in the Data Protection Legislation.</p>
Schedule 3 - Glossary and interpretations	<p><b>Data Loss Event</b></p> <p>Any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Framework Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Framework Agreement, including any Personal Data Breach.</p>
Schedule 3 - Glossary and interpretations	<p><b>Data Protection Impact Assessment</b></p> <p>An assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.</p>
Schedule 3 - Glossary and interpretations	<p><b>Data Protection Legislation</b> <del>or DPA</del></p> <p><del>The Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations about the processing of personal data and privacy, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.</del></p> <p>Data Protection Legislation means:</p> <p>i) all applicable Law about the processing of personal data and privacy; and</p> <p>ii) The Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 including if</p>

	<p>applicable legally binding guidance and codes of practice issued by the Information Commissioner; and</p> <p>iii) to the extent that it relates to processing of personal data and privacy, any Laws that come into force which amend, supersede or replace existing Laws including the GDPR, the (LED Law Enforcement Directive (Directive (EU) 2016/680) and any applicable national implementing Laws as amended from time to time including the DPA 2018 [subject to Royal Assent].</p>
Schedule 3 - Glossary and interpretations	<p><b>Data Subject</b></p> <p>Takes the meaning given in the Data Protection Legislation.</p>
Schedule 3 - Glossary and interpretations	<p><b>DPA 2018</b></p> <p>Data Protection Act 2018.</p>
Schedule 3 - Glossary and interpretations	<p><b>GDPR</b></p> <p>The General Data Protection Regulation (Regulation (EU) 2016/679).</p>
Schedule 3 - Glossary and interpretations	<p><b>LED Law Enforcement Directive (Directive (EU) 2016/680).</b></p>
Schedule 3 - Glossary and interpretations	<p><b>Personal Data</b></p> <p><del>As described in the Data Protection Act 1998</del> Takes the meaning given in the Data Protection Legislation.</p>
Schedule 3 - Glossary and interpretations	<p><b>Processor</b></p> <p>Takes the meaning given in the Data Protection Legislation.</p>
Schedule 3 - Glossary and interpretations	<p><b>Protective Measures</b></p> <p>Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and</p>

	regularly assessing and evaluating the effectiveness of such measures adopted by it.
Schedule 3 - Glossary and interpretations	<b>Subprocessor</b> Any third party appointed to process Personal Data on behalf of the Supplier under this Framework Agreement.

## Call-off contract

### Clause

Part A - Order Form - <b>Additional buyer terms</b>	<b>Personal Data and Data Subjects</b>  Will Schedule 7 – Processing, Personal Data and Data Subjects be used Y/N
2. Incorporation of terms	<del>8.57 to 8.62 (Data protection and disclosure)</del>
Clause 10.1	Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the <del>Data Protection Act (DPA)</del> <b>Data Protection Legislation</b> or under incorporated Framework Agreement clauses 8.83 to 8.91. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.
New Clause 33	<b>33.</b>  <b>Data Protection Legislation (GDPR)</b>  <b>33.1</b>  <b>The Parties will comply with the Data Protection Legislation and agree that the Buyer is the Controller and the Supplier is the Processor. The only processing the Supplier is authorised to do is listed at Schedule 7 unless Law requires otherwise (in which</b>

case the Supplier will promptly notify the Buyer of any additional processing if permitted by Law).

### 33.2

The Supplier will provide all reasonable assistance to the Buyer to prepare any Data Protection Impact Assessment before commencing any processing (including provision of detailed information and assessments in relation to processing operations, risks and measures) and must notify the Buyer immediately if it considers that the Buyer's instructions infringe the Data Protection Legislation.

### 33.3

The Supplier must have in place Protective Measures, which have been reviewed and approved by the Buyer as appropriate, to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.

### 33.4

The Supplier will ensure that the Supplier Personnel only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier Personnel with access to Personal Data, including by ensuring they:

i) are aware of and comply with the Supplier's obligations under this Clause;

ii) are subject to appropriate confidentiality undertakings with the Supplier or relevant Subprocessor

iii) are informed of the confidential nature of the Personal Data and don't publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract

iv) are given training in the use, protection and handling of Personal Data.

### 33.5

The Supplier will not transfer Personal Data outside of the European Economic Area unless the prior written consent of the Buyer has been obtained and

i) the Buyer or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Buyer;

ii) the Data Subject has enforceable rights and effective legal remedies;

iii) the Supplier 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 Buyer in meeting its obligations); and

iv) the Supplier complies with any reasonable instructions notified to it in advance by the Buyer with respect to the processing of the Personal Data.

### 33.6

The Supplier will delete or return Buyer's Personal Data (including copies) if requested in writing by the Buyer at the End or Expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.

### 33.7

The Supplier will notify the Buyer immediately if it receives any communication from a third party relating to the Parties' obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide the Buyer with full and ongoing assistance in relation to each Party's obligations under the Data Protection Legislation in accordance with any timescales reasonably required by the Buyer.



	<p><b>33.8</b></p> <p>The Supplier will maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:</p> <ul style="list-style-type: none"> <li>i) the Buyer determines that the processing is not occasional;</li> <li>ii) the Buyer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and</li> <li>iii) the Buyer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.</li> </ul> <p><b>33.9</b></p> <p>Before allowing any Subprocessor to process any Personal Data related to this Call-Off Contract, the Supplier must obtain the prior written consent of the Buyer, and shall remain fully liable for the acts and omissions of any Subprocessor.</p> <p><b>33.10</b></p> <p>The Buyer may amend this Call-Off Contract on not less than 30 Working Days' notice to the Supplier to ensure that it complies with any guidance issued by the Information Commissioner's Office.</p>
Schedule 6 - Glossary and interpretations	<p><b>Controller</b></p> <p>Takes the meaning given in the Data Protection Legislation.</p>
Schedule 6 - Glossary and interpretations	<p><b>Data Loss Event</b></p> <p>Any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Call-Off Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Call-Off Contract, including any Personal Data Breach.</p>

Schedule 6 - Glossary and interpretations	<p><b>Data Protection Impact Assessment</b></p> <p>An assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.</p>
Schedule 6 - Glossary and interpretations	<p><b>Data Protection Legislation <del>or DPA</del></b></p> <p><del>The Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.</del></p> <p>Data Protection Legislation means:</p> <p>i) all applicable Law about the processing of personal data and privacy; and</p> <p>ii) The Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 including if applicable legally binding guidance and codes of practice issued by the Information Commissioner; and</p> <p>iii) to the extent that it relates to processing of personal data and privacy, any Laws that come into force which amend, supersede or replace existing Laws including the GDPR, the LED and any applicable national implementing Laws as amended from time to time including the DPA 2018 [subject to Royal Assent].</p>

Schedule 6 - Glossary and interpretations	<b>Data Subject</b> Takes the meaning given in the Data Protection Legislation.
Schedule 6 - Glossary and interpretations	<b>DPA 2018</b> Data Protection Act 2018
Schedule 6 - Glossary and interpretations	<b>GDPR</b> The General Data Protection Regulation (Regulation (EU) 2016/679).
Schedule 6 - Glossary and interpretations	<b>LED</b> Law Enforcement Directive (Directive (EU) 2016/680).
Schedule 6 - Glossary and interpretations	<b>Personal Data</b> Takes the meaning given in the Data Protection Legislation.
Schedule 6 - Glossary and interpretations	<b>Personal Data Breach</b> Takes the meaning given in the Data Protection Legislation.
Schedule 6 - Glossary and interpretations	<b>Processor</b> Takes the meaning given in the Data Protection Legislation.
Schedule 6 - Glossary and interpretations	<b>Protective Measures</b> Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.

Schedule 6 - Glossary and interpretations	<p><b>Subprocessor</b></p> <p>Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.</p>
New Schedule 7: Processing, Personal Data and Data Subjects	<p><b>Subject matter of the processing:</b></p> <p>[This should be a high level, short description of what the processing is about ie its subject matter]</p> <p><b>Duration of the processing:</b></p> <p>[Clearly set out the duration of the processing including dates]</p> <p><b>Nature and purposes of the processing:</b></p> <p>[Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the processing means any operation 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 of data (whether or not by automated means) etc]</p> <p>The purpose might include eg: employment processing, statutory obligation, recruitment assessment etc]</p> <p><b>Type of Personal Data:</b></p> <p>[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]</p> <p><b>Categories of Data Subject:</b></p> <p>[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]</p> <p><b>Plan for return or destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data:</b></p> <p>[Describe how long the data will be retained for and how it will be returned or destroyed]</p>