The contract variation for Digital Outcomes and Specialists 2

The Crown Commercial Service (CCS) has made some minor changes to the framework agreement and call-off contract (reference RM1043iv) because of the new General Data Protection Regulation (GDPR).

Framework agreement

Clause	Change
9.32.1	The Supplier will comply with any notification requirements under the Data Protection ~~Act 1998~~ Legislation and both Parties will observe their obligations under it.
9.32.2	~~Each Party will:~~ ~~• treat all the other Party's Confidential Information as confidential and safeguard it accordingly~~ ~~• not disclose the other Party's Confidential Information to any other person without the prior and written consent of the other Party~~ The Parties will comply with the Data Protection Legislation and agree that 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: i) restricted to operations that are strictly necessary for the management/administration of this Framework Agreement; and ii) 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.

9.32.3	~~The above clauses will not apply to any Confidential Information in the following circumstances:~~ ~~• it is public knowledge~~ ~~• it was in the possession of the receiving Party, without restriction as to its disclosure, before receiving it from the disclosing Party~~ ~~• it is received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure~~ ~~• it is information independently developed without access to the Confidential Information~~ ~~• it must be disclosed following a statutory or legal obligation~~ ~~• it is disclosed on a confidential basis to a professional adviser~~ 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.
9.32.4	~~It is recommended that Suppliers and Buyers sign a non-disclosure agreement before they share any Confidential Information.~~ 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.
9.32.5	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.
9.32.6	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.
9.32.7	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.
9.32.8	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 ● 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 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 ● obtain the prior written consent of CCS before allowing any Subprocessor to process any Personal Data related to this Framework Agreement 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 9.32.1 to 9.32.8.

9.32.9	Each Party will: ● treat all the other Party's Confidential Information as confidential and safeguard it accordingly ● not disclose the other Party's Confidential Information to any other person without the prior and written consent of the other Party
9.32.10	The above clauses will not apply to any Confidential Information in the following circumstances: ● it is public knowledge ● it was in the possession of the receiving Party, without restriction as to its disclosure, before receiving it from the disclosing Party ● it is received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure ● it is information independently developed without access to the Confidential Information ● it must be disclosed following a statutory or legal obligation ● it is disclosed on a confidential basis to a professional adviser
9.32.11	It is recommended that Suppliers and Buyers sign a non-disclosure agreement before they share any Confidential Information.
Section 10 - Defined Terms	**Controller** Takes the meaning given in the Data Protection Legislation.
Section 10 - Defined Terms	**Data Loss Event** 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.
Section 10 - Defined Terms	**Data Protection Impact Assessment** An assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Section 10 - Defined Terms	**Data Protection Legislation** Data Protection Legislation means: i) all applicable Law about the processing of personal data and privacy; and 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 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].
Section 10 - Defined Terms	**Data Subject** Takes the meaning given in the Data Protection Legislation.
Section 10 - Defined Terms	**DPA 2018** Data Protection Act 2018.
Section 10 - Defined Terms	**GDPR** The General Data Protection Regulation (Regulation (EU) 2016/679).
Section 10 - Defined Terms	**LED** Law Enforcement Directive (Directive (EU) 2016/680).
Section 10 - Defined Terms	Personal Data ~~As described in the Data Protection Act 1998~~ Takes the meaning given in the Data Protection Legislation.

Section 10 - Defined Terms	**Personal Data Breach** Takes the meaning given in the Data Protection Legislation.
Section 10 - Defined Terms	**Processing** This has the meaning given to it under the Data Protection Legislation but, for the purposes of this Framework Agreement and Call-Off Contract, it will include both manual and automatic processing. 'Process' and 'processed' will be interpreted accordingly.
Section 10 - Defined Terms	**Processor** Takes the meaning given in the Data Protection Legislation.
Section 10 - Defined Terms	**Protective Measures** 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.
Section 10 - Defined Terms	**Subprocessor** Any third party appointed to process Personal Data on behalf of the Supplier under this Framework Agreement.

Call-off contract

Clause	Change

Part B - The Schedules New Schedule 9: Processing, Personal Data and Data Subjects	**Subject matter of the processing:** [This should be a high level, short description of what the processing is about ie its subject matter] **Duration of the processing:** [Clearly set out the duration of the processing including dates] **Nature and purposes of the processing:** [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. The purpose might include eg: employment processing, statutory obligation, recruitment assessment etc] **Type of Personal Data:** [Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc] **Categories of Data Subject:** [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] **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:** [Describe how long the data will be retained for, how it will be returned or destroyed]

Part C - Terms and conditions 13.8	At the end of the term of the Call-Off Contract, the Buyer grants to the Supplier a licence to use the Project-Specific IPRs (excluding any information which is the Buyer's Confidential Information or which is subject to the Data Protection Legislation ~~Act (DPA))~~ on the terms of the Open Government Licence v3.0.
14.1	~~The Supplier shall comply with any notification requirements under the DPA and both Parties will duly observe all their obligations under the DPA which arise in connection with the Framework Agreement or under the Call-Off Contract.~~ 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 9 unless Law requires otherwise (in which case the Supplier will promptly notify the Buyer of any additional processing if permitted by Law).
14.2	~~Where the Supplier is processing Buyer Data or Other Contracting Bodies' Personal Data, the Supplier shall ensure that it has in place appropriate technical and organisational measures to ensure the security of the Authority and Other Contracting Bodies' Personal Data (and to guard against unauthorised or unlawful processing or accidental loss, destruction of or damage to the Buyer Data and the Other Contracting Bodies' Personal Data.~~ 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.

14.3	~~The Supplier shall provide the Buyer and/or Other Contracting Body with such information as the Buyer and/or Other Contracting Body may reasonably request to satisfy itself that the Supplier is complying with its obligations under the DPA including:~~ ~~to promptly notify the Buyer and/or Other Contracting Body of any breach of the security measures to be put in place pursuant to this Clause; and~~ ~~to ensure that it does not knowingly or negligently do or omit to do anything which places the Buyer and/or Other Contracting Body in breach of its obligations under the DPA and~~ ~~not to cause or permit to be processed, stored, accessed or otherwise transferred outside the European Economic Area any Buyer Data or Other Contracting Body Personal Data supplied to it by the Buyer or Other Contracting Body without approval.~~ 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.
14.4	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

14.5	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 the following conditions are met: (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
14.6	The Supplier will delete or return the Buyer's Personal Data (including copies) if requested in writing by the Buyer at the termination or expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.
14.7	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.

14.8	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: i) the Buyer determines that the processing is not occasional; 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 iii) the Buyer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
14.9	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.
14.10	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.
15.9	The Supplier will provide, at the request of CCS or the Buyer, any information relating to the Supplier's compliance with its obligations under the Data Protection ~~Act~~ Legislation. The Supplier will also ensure that it does not knowingly or negligently fail to do something that places CCS or any Buyer in breach of its obligations of the Data Protection ~~Act~~ Legislation. This is an absolute obligation and is not qualified by any other provision of the Call-Off Contract.
44. Defined Terms	**Controller** Takes the meaning given in the Data Protection Legislation.
44. Defined Terms	**Data Loss Event** 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.

44. Defined Terms	**Data Protection Impact Assessment** An assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
44. Defined Terms	**Data Protection Legislation** Data Protection Legislation means: i) all applicable Law about the processing of personal data and privacy; and 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 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].
44. Defined Terms	**Data Subject** Takes the meaning given in the Data Protection Legislation.
44. Defined Terms	**DPA 2018** Data Protection Act 2018.
44. Defined Terms	**GDPR** The General Data Protection Regulation (Regulation (EU) 2016/679).
44. Defined Terms	**LED** Law Enforcement Direction (Directive (EU) 2016/680).

44. Defined Terms	**Personal Data** ~~As described in the Data Protection Act 1998~~ Takes the meaning given in the Data Protection Legislation.
44. Defined Terms	**Personal Data Breach** Takes the meaning given in the Data Protection Legislation.
44. Defined Terms	**Processing** This has the meaning given to it under the Data Protection Legislation but, for the purposes of this Framework Agreement and Call-Off Contract, it will include both manual and automatic processing. 'Process' and 'processed' will be interpreted accordingly.
44. Defined Terms	**Processor** Takes the meaning given in the Data Protection Legislation.
44. Defined Terms	**Protective Measures** 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.
44. Defined Terms	**Subprocessor** Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.