

CHANGE CONTROL NOTE

Contract Change Note

Contract Change Note Number	CCN 1
Contract Reference Number & Title	CQC ICTC 801 Omni Channel Contact Centre Software
Variation Title	Contract extension and inclusion of Data Protection Impact Assessment (DPIA) for Speech Analytics.
Number of Pages	22

WHEREAS the Contractor and the Authority entered into a contract for the provision of Omni Channel Contact Centre Software Licenses dated 2nd April 2020 (the "Original Contract") and now wish to amend the Original Contract.

IT IS AGREED as follows

1. The Original Contract shall be amended as set out in this Change Control Notice:

Change	Care Quality Commission
Summary of change	<p>The Authority wishes to vary the terms of the G-Cloud 11 Call-Off Contract – Order Form by executing the contract extension arrangement and the inclusion of Data Protection Impact Assessment (DPIA) for Speech Analytics Software.</p> <p><u>Extension</u></p> <p>The Authority wishes to vary the terms of the G-Cloud 11 Call-Off Contract – Order Form by extending the contract for a further 24 months in accordance to Part A – Order form of the contract.</p> <p>The contract extension will take effect from 1st April 2022 and the new expiry date will 31st March 2024.</p>

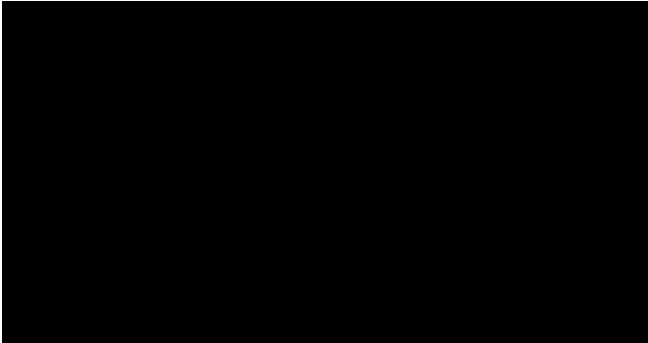
	<p>*** The prices above exclude VAT</p> <p><u>Annex 1 details Data Protection Impact Assessment (DPIA) Process for Speech Analytics</u></p> <p>The inclusion of DPIA document for Speech analytics software as using 3rd party third party to complete the call transcriptions.</p>
Reason for Change	<p>The Authority wishes to vary the terms of the G-Cloud 11 Call-Off Contract – Order Form by executing the contract extension arrangement and the inclusion of Data Protection Impact Assessment (DPIA) for Speech Analytics Software.</p> <p>The original terms and conditions will apply throughout the life of the contract and this contract change notice and any future contract change notices.</p>

Revised Contract Price	Original Contract Value	£718,830.00 excluding VAT £862,696.80 including VAT
	Previous Contract Changes	£ N/A
	Contract extension charges	£929,797.00 excluding VAT £1,115,696.00 including VAT
	New Contract Value	£1,648,627.00 excluding VAT £1,978,392.80 including VAT
Revised Payment Schedule	Payment annual in advance	
Revised Specification	The Authority wishes to vary the terms of the G-Cloud 11 Call-Off Contract – Order Form by executing the contract extension arrangement and the inclusion of Data Protection Impact Assessment (DPIA) for Speech Analytics Software.	
Revised Term/Contract Period	The original terms and conditions will still apply for the life of the contract.	
Change in Contract Manager(s)	N/A	
Other Changes	N/A	

2. Save as herein amended all other terms of the Original Contract shall remain effective.
3. This Change Control Notice shall take effect on 1st April 2022 of which both the Authority and the Contractor have communicated acceptance of its terms.

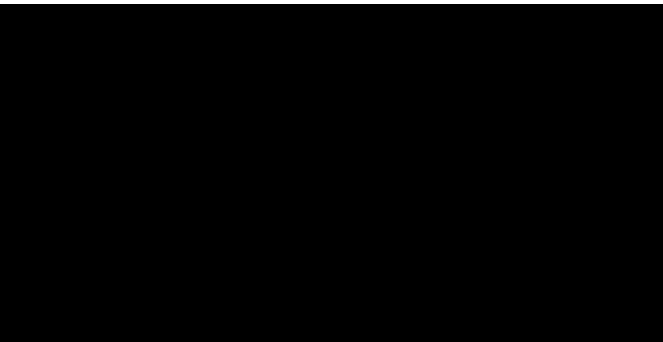
SIGNED for and on behalf of **CARE QUALITY COMMISSION**

Authorised Signatory:

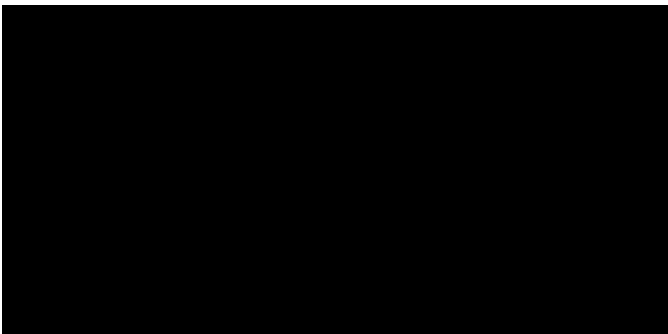


SIGNED for and on behalf of **PUZZEL LTD**

Authorised Signatory 1:



Authorised Signatory 2:



Annex 1 - Data Protection Impact Assessment (DPIA) Process for Speech Analytics

DATA PROTECTION IMPACT ASSESSMENT (DPIA) PROCESS

May 2018

Background

Completing a Data Protection Impact Assessment (DPIA) is a legal requirement under Article 35 of the General Data Protection Regulation (GDPR) where the intended processing of information carries a high risk to the rights and freedoms of living persons. High risks may arise from the use of new technologies, from processing sensitive information such as health data, from processing high volumes of information about identifiable persons, or where we are monitoring or making decisions about people.

Completing a DPIA also helps us to ensure that we are protecting the privacy, dignity, rights and freedoms of people whose information we use. In turn this helps us to maintain trust in CQC.

Process

The Confidentiality, Privacy and Security Advisor [REDACTED] will advise and assist you throughout the DPIA process.

Step 1: – Deciding whether a DPIA is required

This is the responsibility of the project lead.

Note: For the purposes of the DPIA process, the term 'project lead' may refer to the person with lead responsibility for a formal project or could simply mean the person with day to day responsibility for carrying out a specified piece of work. Likewise, references to 'the project' should be considered as the defined piece of work that is being assessed, rather than necessarily being a formally defined project.

A DPIA is required for:

- Formal projects, or
- The introduction of new policies or operational processes, or
- Changes to existing policies and processes, or
- New agreements or arrangements for sharing or disclosing information to external organisations, or
- Organisational change, or
- Introduction of new systems, or
- The use of new technologies, or
- Significant change to the operation or use of existing systems, or
- Changes to information security, to the storage and handling of information, or to the retention periods or disposal processes for information

Where:

- Those changes relate to the processing (obtaining, recording, storage, use, sharing, alteration, deletion or destruction) of personal data (information about living individuals who can be identified by that data, or who CQC otherwise has the means to identify), or
- Those changes relate to the combining of anonymised or aggregated data sets where this carries any risk that individuals could therefore be re-identified from that data, or
- The intention is to monitor or make decisions about living persons, or
- Those change carry a risk to the privacy, rights, welfare, safety or legitimate interests of living persons.

If in doubt, consult the Information Rights Manager.

Step 2: - Complete Part 1 of the form (Project details)

This is the responsibility of the project lead. Advice and assistance can be accessed as needed.

Completion of the form should not be delayed where the required information for a field is unknown, undecided or unclear. Completing and signing off a DPIA is likely to be an iterative process so the form can be updated at a later stage, as required.

Step 3: - Complete Part 2 of the form (Screening)

This is the responsibility of the project lead. Advice and assistance can be accessed as needed.

If the answers to all screening questions are 'No', it is likely that further assessment will not be required. The Information Rights Manager will record the form on the DPIA log.

Step 4: Complete Part 3 of the form (Full DPIA)

This is the responsibility of the project lead but will usually be conducted collaboratively with Information Rights, Security and KIM colleagues.

Necessity: This section should be used to explain why it is necessary to use personal data to achieve the purpose of the project. Where personal data is not being used, you can simply mark this section as 'N/A'.

Where the processing of personal data is required, explain why. Why are alternative approaches that do not involve processing personal data not possible or practicable?

Evaluation and consultation: Explain what you have done to understand the risks, issues and impacts relating to the project. This may be an internal evaluation with CQC colleagues and/or an external consult with people whose privacy is likely to be impacted, or who may be placed at risk or otherwise impacted by the project. If people who are likely to be affected are not being consulted, you should explain why.

Information risks and issues assessment: You should not delay completion and submission of the form because you have not fully assessed the risks, these can be updated as the DPIA process proceeds.

Impact Scores
5 - Very High
4 - High
3 - Medium
2 - Low
1 - Very Low

Likelihood Scores
5 - Very High
4 - High
3 - Medium
2 - Low
1 - Very Low

Current risk is calculated as likelihood x impact to give a score between 1 and 25.

Once this section has been completed, submit the form to [REDACTED]

Step 5: - Assessment

The Information Rights Manager will establish which lawful bases for processing personal data and sensitive personal apply (where relevant). Processing of personal data cannot lawfully be carried on without establishing a lawful basis to do so.

The Information Rights Manager, Information Security Manager and Knowledge and Information Manager (or delegated members of their teams) will refer questions to the project lead as needed and will review the form and return it for amendment as required (e.g. where additional risks have been identified).

Once the form has been amended and resubmitted as required, the Information Rights Manager will – in consultation with the Information Security Manager and Knowledge and Information Manager make a recommendation as to whether the project should be approved, as to the overall level of residual risk to privacy / data subjects, and as to whether these risks are proportionate to the purpose of the project.

Step 6: - Sign off

The Information Rights Manager will pass the form to the Data Protection Officer (DPO) who will review the form and discuss as needed. The DPO will then add her own recommendation and the Information Rights Manager will forward the form for sign-off.

Final sign off for all assessments will be by the Senior Information Risk Owner (SIRO) or, in his absence, the Deputy SIRO.

Any assessment involving the processing of personal data relating to people who use health and social care services must also be signed off by the Caldicott Guardian, or in his absence, his appointed deputy.

Where a high risk to privacy or data subjects has been identified and cannot be adequately mitigated, the proposed processing must be referred to the Information Commissioner's Office (ICO), and must receive their approval before SIRO sign off.

Step 6: - Ownership and management of risk

Information risks identified during the DPIA process are the responsibility of the project lead and must be managed accordingly. High and medium information risks will be reported to the Information Governance Group (IGG). The IGG may decide to enter these risks onto the Information Risk Register (IRR), to update an existing risk on the IRR, and/or to ask the project lead to report on the management of those risks.

Step 7: - Updates and changes

The project lead is responsible for identifying any significant changes to the project, to the processing of personal data, or to risks and issues following DPIA sign-off.

These should be recorded in Part 5 of the DPIA and forwarded to the Information Rights Manager, who will seek the recommendation of the DPO and the sign-off of the SIRO.

Step 8: - Review

The SIRO will set a date for review for all DPIAs that he signs off. All DPIAs must be reviewed at least every 3 years.

A review of the DPIA may also be undertaken where there have been multiple or very significant changes following initial sign-off.

The review will be conducted by the project lead, working with the Confidentiality, Privacy and Security Advisor (CPSA). The updated form will then follow the process from step 5.

DATA PROTECTION IMPACT ASSESSMENT (DPIA) FORM

Please consult the Information Rights Team [REDACTED] Information Security Team [REDACTED]
and Knowledge & Information Management (KIM) Team [REDACTED] as needed in completing this form

Part 1 – Project details

Title of project:	[REDACTED]
Project sponsor:	[REDACTED]
Project lead:	[REDACTED]
Project start date:	14 July 2021
Project end date:	31 August 2021
'Go live' date for system or business changes:	1 November 2021

Business purpose for project or proposed change:

Briefly describe what the proposed work is attended to achieve, and how this will support CQC in performing its functions.

As part of the NCSC Omni project we are launching the Speech Analytics functionality within our existing Workforce management system.

This software will automatically transcribe call recordings from voice into text allowing further analysis of call drivers and customer experience. In order to ensure the system transcribes call accurately a sample of 50 hours of calls received into CQC need to be manually transcribed. CQC does not have resource to complete this activity, so we would like to outsource this task to STW.

Information flows:

Describe what personal data (information relating to individuals, whether they are identifiable or not) will be used. Where will this information be obtained from, where will it be stored/processed, and where will it (or information generated from it) be sent to? (Enter 'N/A' if project does not involve personal data)

Note: if the information flows are not yet known, please say so. Do not delay completion and submission of the form.

- A) STW will listen to 50 hours of call recordings. To take a good enough sample, 30 hours was recommended, but CQC have decided that 50 is more appropriate due to the complexity of calls that we deal with. The calls that are being transcribed are conversations between the Customer and the NCSC Customer Services Agent.
- B) STW will transcribe the calls into a text file.
- C) The transcribed information will then be sent to Verint and CQC.

Data processors:

Will any external organisation process personal data on behalf of CQC? If so, provide a) the name of the company (if known at this time), b) a description of the processing they will undertake, c) a description of controls that will be in place (contracts etc.), d) security due diligence checks carried out - security certifications e.g. Cyber Essentials, ISO27001.

Note: if the use of, or identity of, data processors are not yet known, please say so. Do not delay completion and submission of the form.

Third parties involved:

- Verint – A sub-contractor of Puzzel and this is the system that CQC staff use

- Puzzel – CQC have a contract with Puzzel. Puzzel sub-contract various parts of the work.
- Support to win (STW). A sub-contractor of Puzzel

STW:

- STW teams work in a Microsoft environment and all files are stored in Teams as the information is highly sensitive. A private Microsoft teams channel is used solely for the project. Only delegates on the project can access the recordings. As per STW's GDPR processes, they delete all information at the project handover stage. Within the SFTP environment, the information is removed after 7 days as per Puzzel's policies.
- All STW staff working on the project have undergone GDPR certification and are aware of implications of any data breaches. STW have processes for data breaches and security breaches.
- All work undertaken by STW staff will be carried out on work devices.
- Access to the SFTP site is via a VPN.
- The security team have reviewed STW's information security policy and privacy policy.

Contractual agreement:

CQC have a contract with Puzzel. In order for this work to be carried out, a contract variation will be made to this contract to allow the transcription service to be carried out by STW – this also includes a data processing agreement to be entered into by CQC and Puzzle. There is a commercial General Services Agreement in place between Puzzel and STW.

The contract variation has not been completed yet, this is subject to the DPIA approval.

Notifying data subjects:

Does the proposed processing of personal data fall within the scope of our existing privacy notices? If not, how will we notify data subjects of the processing? (Enter 'N/A' if project does not involve personal data)

Note: if a decision on notifying data subjects has not yet been made, please say so. Do not delay completion and submission of the form.

To complete the call transcriptions, a selection of call recordings will be downloaded from Verint which will include a full range of queries handled by NCSC, this could include confidential and/or personal information.

Personal data that may be requested by CQC during the call includes; names, addresses, contact details (phone number and email) and employer details. Customers may also share personal information relating to their experience of health and social care services such as details of their treatment or health conditions. When a customer contacts CQC they are aware of our privacy notice as part of the IVR, they hear the following message:

Welcome to the Care Quality Commission. Please be aware calls may be recorded or monitored for training purposes.

Personal data will be processed and protected in accordance with the General Data Protection Regulation. If you would like more information about how and why we process personal data and your own data protection rights, this can be found on our website – www.cqc.org.uk or by asking your call advisor.

Transcriptions will be retained in Verint in line with our existing retention policy for call recordings (4 Months)

As part of our IVR customers are advised our privacy notice and are informed that the calls are recorded for training and monitoring purposes.

All CQC contact centre staff have given consent for their voices to be recorded, along with all customers are informed that the calls are recorded for training and monitoring purposes.

Part 2 – Screening

SCREENING QUESTION	(Delete as applicable)		
Question 1: Will the proposed system or process be used to evaluate, score, profile or make predictions <i>about living persons</i> ?	NO		
Question 2: Will the proposed system or process be used for automated decision making <i>about living persons</i> ?	NO		
Question 3: Will the proposed system or process be used for the systematic monitoring or control <i>of living persons</i> ?	NO		
Question 4: Will the proposed system or process involve processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health condition or needs, sex life, sexual orientation, or criminal convictions <i>of identifiable, living persons</i> ?		YES	
Question 5: Will the proposed system or process involve the processing of genetic data or biometric data (e.g. fingerprints, iris scans, tissue samples, similarity scores)?	NO		
Question 6: Will the proposed system or process involve the processing of information relating to more than 1000 <i>identifiable people</i> ?	NO		
Question 7: Will the proposed system or process involve the processing of a large or disparate amount of data items <i>relating to an individual person</i> ?	NO		
Question 8: Will the proposed system or process involve the linking or combination of multiple (more than one) existing datasets?	NO		
Question 9: Will the proposed system or process <i>specifically</i> involve processing information about identifiable and vulnerable persons (e.g. children, the elderly, people with mental health conditions)?		YES	
Question 10: Will the proposed system or process involve the use of new technologies, or involve the innovative use of technological or organisational solutions that will collect or use personal data in novel and unexpected ways?	NO		
Question 11: Will the proposed system or process involve the transfer, storage or sharing of personal data outside of the UK (including via cloud storage)?		YES	
Question 12: Will the proposed system or process interfere with the rights of living individuals – including their right to be notified of the processing of their personal data (i.e. if new data will be collected without directly notifying those individuals), and their right to object to such processing?	NO		

If all answers are '**No**', submit the form now to [REDACTED]

If any answers are '**Yes**' please complete Part 3 of this form.

Part 3 – Full Data Protection Impact Assessment

(This section only needs to be completed if you answered 'yes' to any of the Part 2, screening questions).

Necessity:

Briefly explain why it is necessary to use the personal data in order to achieve the purpose. (Enter 'N/A' if project does not involve personal data).

Speech analytics software requires a large sample baseline dataset in order to enable it to effectively transcribe our future calls. This dataset needs to include all potential terminology, phrases and key words frequently used in interactions with CQC.

This needs to be outsourced as the transcription of calls required was estimated to take 10 FTE at least two weeks to complete. We currently do not have that resource available. It is not possible for us to redact the calls without significant manual intervention, this is not a viable option for us.

Evaluation and consultation:

Explain how the potential impact on personal privacy, and any risks relating to the information (e.g. security risks, legal compliance), have been (or will be) assessed. How will you understand what the potential impacts and risks are? For potentially high risk activities, consultation is recommended – if you will not consult with people who are likely to be affected, explain why not.

Any personal information disclosed during the call is done so with the customer knowing that the call is recorded, and any information provided could be used to deliver our regulatory purpose.

A small quantity of call recordings will be shared with a third party (STW) to transcribe the calls.

Information risk and issues assessment:

Where potential privacy impacts have been identified, the risk of those impacts materialising should be included. Risk assessment should also include: risks to confidentiality (e.g. security risks), legal risks (e.g. potential breaches of data protection laws), regulatory risks (e.g. impact on effectiveness due to data quality issues).

Risk/issue	Controls & mitigations currently in place	Likelihood (1-5)	Impact (1-5)	Current risk (1-25)	Planned controls and mitigations (in	Anticipated risk (1-25)
Confidential information is inappropriately retained or disclosed by the third party	<ul style="list-style-type: none"> The security team have reviewed STW's security controls (and read their information security policy and privacy policy) A retention period has been agreed. 	2	3	6	<ul style="list-style-type: none"> A contract change notification will be put in place, and the contract contains a data processing agreement. This is subject to the DPIA being approved. 	Medium
Call recordings may be shared before customers requests to be forgotten have been processed.	<ul style="list-style-type: none"> A privacy notice is outlined at the start of the call. We will only share calls with third party that are over a week old. This will give us time to process requests that customers do not wish there calls to be used. 	1	2	2		Low
	•				•	
	•				•	
	•				•	

Once completed, submit the form to [REDACTED]

Part 4 - Assessment

To be completed by the Information Rights Manager

Lawful basis for processing: To be completed by Information Rights Manager	
General Data Protection Regulation	
<p>Article 6 lawful basis:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Consent (Art 6, para 1(a)) <input type="checkbox"/> Contract (Art 6, para 1(b)) <input type="checkbox"/> Legal obligation (Art 6, para 1(c)) <input type="checkbox"/> Vital interests (Art 6, para 1(d)) <input checked="" type="checkbox"/> Public interest (Art 6, para 1(e)) <input checked="" type="checkbox"/> Exercise of official authority (Art 6, para 1(e)) <input type="checkbox"/> Legitimate interests (Art 6, para 1(f)) 	<p>Article 9 lawful basis (for special categories of personal data)</p> <ul style="list-style-type: none"> <input type="checkbox"/> Explicit consent (Art 9, para 2(a)) <input type="checkbox"/> Employment rights/obligations (Art 9, para 2(b)) <input type="checkbox"/> Vital interests (Art 9, para 2(c)) <input type="checkbox"/> Made public by data subject (Art 9, para 2(e)) <input type="checkbox"/> Exercise or defence of legal claims (Art 9, para 2(f)) <input checked="" type="checkbox"/> Substantial public interest / basis in law (Art 9, para 2(g)) <input checked="" type="checkbox"/> Health or social care / duty of secrecy (Art 9, para 2(h)) <input checked="" type="checkbox"/> Public health / duty of secrecy (Art 9, para 2(i)) <input type="checkbox"/> Archiving / basis in law (Art 9, para 2(j))
<p>Balance of interests (for public interest/legitimate interests):</p>	
Recommendation of the Information Rights Manager:	
In the absence of the IRM, this DPIA is being passed on to the DPO & SIRO.	
Privacy impact and risk to data subjects assessment:	Medium
<p>Assessment of proportionality:</p> <p>Confidentiality, Privacy & Security Advisor comments – Recommends approval. The project team have considered the impact on privacy, the security team have reviewed the controls being put in place by the third parties and are satisfied with it, and only a sample of information will be shared. A data processing agreement is also being put in place.</p>	

Part 5 - SIGN OFF

Recommendation of the Data Protection Officer:
This processing is limited, lawful and appropriate. I recommend approval (25/10/21)

	REQUIRED (Y/N)	DATE of APPROVAL
CALDICOTT APPROVAL:	Yes	Approved on 28/10/21
SIRO APPROVAL:	Yes	SIRO approval on 21/10/21 Deputy SIRO approval on 22/10/21

If recommendation of the Data Protection Officer is not followed, explain reasons:

Date for review:	31/10/2022
------------------	------------

Part 5 – Post sign-off changes

[illegible]