Crown Commercial Service

G-Cloud 12 Call-Off Contract

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:

G-Cloud 12 Call-Off Contract 1

Part A: Order Form 2

Schedule 1: Services 12

Schedule 2: Call-Off Contract charges 21

Part B: Terms and conditions 23

Schedule 3: Collaboration agreement 43

Schedule 4: Alternative clauses 56

Schedule 5: Guarantee 60

Schedule 6: Glossary and interpretations 69

Schedule 7: GDPR Information 81

Schedule 8: Supplier Terms 90

Part A: Order Form

Buyers must use this template order form as the basis for all call-off contracts and must refrain from accepting a supplier's prepopulated version unless it has been carefully checked against template drafting.

Digital Marketplace service ID number	3383 1255 3726 793
Call-Off Contract reference	CQC EP&S 003
Call-Off Contract title	Online Participation Platform
Call-Off Contract description	Online crowdsourcing platform to support external engagement of both providers of health and social care services in England and the public that use those services.
Start date	1st November 2021
Expiry date	31st October 2023
Call-Off Contract value	[redacted]
Charging method	BACS
Purchase order number	TBC

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From the Buyer	Care Quality Commission 020 7448 9086 Citygate Gallowgate Newcastle upon Tyne NE1 4PA
To the Supplier	CitizenLab, Meusegemstraat 105 1861 Meise, Belgium, BE 0638.901.287 Company number: [enter number]
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Head of Public Engagement & Involvement

Name: Jill Morrell

Email: jill.morrell@cqc.org.uk

Phone: [redacted]

For the Supplier:

Title: Country Lead UK

Name: Lora Botev

Email: lora.botev@citizenlab.uk

Phone: [redacted]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 1st November 2021 and is valid for 2 years (ending 31st October 2023)
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-off Contract can be extended by the Buyer for 2 period(s) of up to 12 months each, by giving the Supplier 30 days written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud lot	This Call-Off Contract is for the provision of Services under: • Lot 2: Cloud software
G-Cloud services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and set out in schedule 1 below.
Additional Services	**None**
Location	The Services will be delivered to 2 Redman Place, 2nd Floor London, E20 1JQ or such a location the both parties agree in light of UK Government COVID 19 guidance permits.
Quality standards	**Not applicable**
Technical standards:	The technical standards used as a requirement for this Call-Off Contract are: 1. As detailed in the supplier's service definition
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are **Supplier's terms Annex II.2.A: Service Level Agreement (Essential and Standard)**.
Onboarding	Getting started We have developed a thorough on-boarding process to guide you in three phases to the successful launch of your platform and first participation project(s): strategy, preparation and launch. Each phase includes a few workshops to help you and your team get to grips with the platform and boost its adoption rate among your communities. Sessions can be held

	online or face-to-face. We also provide extensive user documentation such as guides and checklists to help you better scope the objectives of your engagement platform. Service documentation: Yes Documentation formats: • HTML • PDF • Other Other documentation formats: • Online knowledge base • Built-in support guide • Case Studies • Blog • Newsletters • In App campaigns
Offboarding	The offboarding plan for this Call-Off Contract is: End-of-contract data extraction: Customers can extract all the data from the platform at any point during the duration of the contract. End-of-contract process: At the end of the contract, CitizenLab will remove the customer's access to the platform and archive all existing projects. The platform and related data is deleted within 12 months. There is no additional cost involved.
Collaboration agreement	Not Applicable
Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed [redacted] The annual total liability for Buyer Data Defaults will not exceed [redacted] of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability for all other Defaults will not exceed the greater of 125% of the Charges payable by the Buyer to

	the Supplier during the Call-Off Contract Term (whichever is the greater).
Insurance	The insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than **30** consecutive days.
Audit	Not Applicable
Buyer's responsibilities	Not Applicable.
Buyer's equipment	Not Applicable

Supplier’s information

Subcontractors or partners

The following is a list of the Supplier’s Subcontractors or Partners.

Name	Type	Opt.	Host location	Purpose	Personal data through	What personal data?
AWS	IaaS	No	EU (Frankfurt)	Data and application server hosting	Hosting	Everything
DigitalOcean	IaaS	No	EU (Frankfurt and Amsterdam)	Supporting web services hosting	Hosting	Everything
Intercom	SaaS	Yes	US (AWS N. Virginia) (SCC)	Communicating with CitizenLab customers	Segment + mail	Only admins and moderators
Salesmachine	SaaS	Yes	EU	Following up on CitizenLab customers to support them	Intercom	Only admins and moderators
Typeform	SaaS	Yes	US (AWS N. Virginia) (SCC)	Rich surveys embedded on the platform	Embedded as iframe	Email is passed as a parameter to the iframe
Facebook Pixel	SaaS	Yes	US (SCC)	Facilitate advertisement campaigns to boost citizen engagement	Segment / Google Tag Manager	User visits
Google Ads	SaaS	Yes	US (SCC)	Facilitate advertisement campaigns to boost citizen engagement	Segment	User visits
Zapier	SaaS	Yes	US (SCC)	Middleware to connect other tools	Intercom	Only admins and moderators
CloudAMQP	IaaS	No	EU (AWS Dublin)	Middleware hosting to connect internal application components	Hosting	Everything
Mailgun	SaaS	No	EU/US (SCC)	Send platform emails	Code integration	email address, name, occasional additional personal data
Satismeter	SaaS	Yes	US (AWS N. Virginia) (SCC)	Collect customer satisfaction score	Segment	Only admins and moderators
Google Tag Manager	Saas	Yes	US (SCC)	Middleware to connect other tools	Segment	User visits

**Mailgun is now entirely stored on EU servers for our UK customers.*

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method	The payment method for this Call-Off Contract is **BACS**.
Payment profile	The payment profile for this Call-Off Contract is monthly in arrears.
Invoice details	The Supplier will issue electronic invoices **monthly** in arrears. The Buyer will pay the Supplier within **30** days of receipt of a valid invoice.
Who and where to send invoices to	Invoices will be sent to Care Quality Commission, T70 payables F175, Phoenix House, Topcliffe Lane Wakefield, West Yorkshire, WF31WE.
Invoice information required	All invoices must include purchase order reference number.
Invoice frequency	Invoice will be sent to the Buyer monthly.
Call-Off Contract value	[redacted]

Call-Off Contract charges	The breakdown of the Charges is: [redacted]

Additional Buyer terms

Performance of the Service and Deliverables	This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones: Not applicable
Guarantee	Not Applicable
Warranties, representations	Not Applicable
Supplemental requirements in addition to the Call-Off terms	Not Applicable
Alternative clauses	Not Applicable

Buyer specific amendments to/refinements of the Call-Off Contract terms	Not Applicable
Public Services Network (PSN)	Not Applicable
Personal Data and Data Subjects	Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.

2.2 The Buyer provided an Order Form for Services to the Supplier.

Signed	Supplier	Buyer
Name	Wietse Van Ransbeeck	Chris Day
Title	Chief Executive Officer	Director of Engagement
Signature	[redacted]	[redacted]
Date	1 November 2021	4 November 2021

Schedule 1: Services

Online public engagement platform for governments

CitizenLab provides organisations with an online resident engagement platform. We enable our customers to engage residents on a continuous basis, manage their input efficiently, and make decisions based on real-time data. All in one place.

CitizenLab Annual: Standard licence valid from 01/11/2021 until 31/10/2024. Dedicated support included throughout the entire license period

Features

- Online consultation toolbox (participation and deliberation)
- Resident input management
- Communication tools
- User and group access management
- Summarisation of resident input using AI
- Custom sign up fields
- Idea classification
- All insights needed for reporting

- API Access
- Location retrieval

Benefits

- Access to a complete toolbox for all your essential consultations
- Keep up to date with public opinion on timely topics
- Leverage resident input to design better informed policies
- Provide a safe online space to contribute to public debates
- Manage all resident input in one central place
- Build automated reports with insights for decision-making
- Hold town hall meetings and focus groups online
- Increase the transparency and accountability of your organisation

Service scope

Software add-on or extension - No

Cloud deployment model - Public cloud

Service constraints - No known constraints.

System requirements - N/A

User support

Email or online ticketing support - Email or online ticketing

Support response times - Within 24 hours on business days.

User can manage status and priority of support tickets - No

Phone support - Yes

Phone support availability - 9 to 5 (UK time), Monday to Friday

Web chat support - Web chat

Web chat support availability - 9 to 5 (UK time), Monday to Friday

Web chat support accessibility standard - WCAG 2.1 AA or EN 301 549

Web chat accessibility testing –

For the built-in chat we make use of Intercom, a software that builds customer relationships through conversational, messenger-based experiences across the customer journey. We have been on a paid subscription of this solid and excellent support chat functionality for 3 years.

Onsite support - Onsite support

Support levels

- Our comprehensive knowledge center (support.citizenlab.co) answers most of your frequently asked questions and offers useful resources to guide you more broadly. For more detailed questions, we are available via email, the built-in chat functionality on your platform or by phone.

CitizenLab provides technical support via a built-in Support Chat system, telephone and e-mail on weekdays from 8:00 to 18:00 GMT ("Support hours"), with the exception of public holidays in the United Kingdom.

The customer can launch a helpdesk ticket during Support Hours by adding it to the chat system, by calling [+44 79 2676 4670] or by emailing at any time [support@citizenlab.co]. CitizenLab will respond to all helpdesk tickets within one (1) business day.

In every pricing plan, an account manager (government success manager) is at your disposal. He or she can bring you in immediate contact with the development team or support desk when necessary.

Support available to third parties - Yes

Onboarding and offboarding

Getting started -

We have developed a thorough on-boarding process to guide you in three phases to the successful launch of your platform and first participation project(s): strategy, preparation and launch. Each phase includes a few workshops to help you and your team get to grips with the platform and boost its adoption rate among your communities. Sessions can be held online or face-to-face. We also provide extensive user documentation such as guides and checklists to help you better scope the objectives of your engagement platform.

Service documentation - Yes

Documentation formats -

- HTML
- PDF
- Other

Other documentation formats

- Online knowledge base
- Built-in support guide
- Case Studies
- Blog
- Newsletters
- In App campaigns

End-of-contract data extraction –

Customers can extract all the data from the platform at any point during the duration of the contract.

End-of-contract process -

At the end of the contract, CitizenLab will remove the customer's access to the platform and archive all existing projects. The platform and related data is deleted within 12 months. There is no additional cost involved.

Using the service

Web browser interface - Yes

Supported browsers

- Internet Explorer 11
- Microsoft Edge
- Firefox
- Chrome
- Safari 9+
- Opera

Application to install - No

Designed for use on mobile devices - Yes

Differences between the mobile and desktop service -

CitizenLab platforms are compliant with WCAG 2.1 AA guidelines (https://www.w3.org/TR/WCAG21/), in line with the European directive on accessibility for government websites and mobile applications.

Service interface - Yes

Description of service interface -

Front-office (visitor & user):
The target audience will see the front-office of the platform. They can browse the content, interact with it or start their own initiatives. It’s made visually attractive, easy to use and structured in such a way that they can explore the content step by step.

Back-office (admin & moderator):
Governments have access to the back-office as well. This part of the platform is structured to align with your internal processes and workflows, and gives you all the options to manage and customise everything that takes place on your platform.

Accessibility standards - WCAG 2.1 AA or EN 301 549

Accessibility testing -

CitizenLab was awarded the AnySurfer label in March 2020, which is in line with WCAG guidelines.

In order to continuously ensure that we still meet this standard when updating the platform and building new functionalities, we have automatic tests in our development environment, using the testing tool 'pa11y'.

In practice, this means the following:

1. The platform is fully navigable with the keyboard. This is important for people with a motor disability for whom navigating with a mouse is difficult or impossible.
2. We give images a so-called 'alt attribute', a self-chosen verbatim description of the image that can be read by screen readers, computers for the visually impaired.
3. We add a description to each button and label all input fields, for the same screen readers.
4. In addition, we work with strong colour contrasts to make the text easy to read for everyone. On our platforms, we offer platform owners the opportunity to choose colours that match their own branding. However, if this compromises the readability of the platform, they receive an accessibility warning. If necessary, we can help you choose the right colours. Users today do not have the ability to change colours.

API - Yes

What users can and can't do using the API -

In addition to the manual export of data, CitizenLab has a well-documented Application Programming Interface (API), so that other applications can exchange data with the software. This API is open so that the data in the platform can be offered in the form of open data. (e.g. for displaying data on a map).

The authentication uses the JWT standard and the login data can easily be obtained from CitizenLab. The documentation contains a complete list of possible operations, with examples. The API is constantly being expanded to unlock new functionalities. The documentation is also consistently kept up to date:

1. Read data
All data from ideas, comments, projects and users are made available for processing by external tools via our documented REST API.

2. Write data
In addition to reading data, the API also offers opportunities to create ideas and approve verifications of citizens. This creates many opportunities for the automated input of content from other systems in the city. One of the possibilities is an integration with the city's agenda software to automatically publish agenda items and reports of the city council or advisory councils on the platform.

API documentation - Yes

API documentation formats - HTML

API sandbox or test environment - Yes

Customisation available - Yes

Description of customisation -

The CitizenLab platform can be customised by each customer to meet their specific needs. The main areas, which customers can personalise are: branding (logos, colours, visuals, etc), languages (the platform is multilingual), topics (to classify resident input), geographic data (map location and zoom levels for instance), registration fields (information requested of users when signing in), webpages (create certain custom pages). Customers also benefit from a modular toolkit that enables them to pick and choose from a toolbox of engagement methods for each specific project.

Scaling

Independence of resources -

The software solution has been built redundantly. The delivery, application and database layers are made up of multiple servers that dynamically distribute the work and can take over from each other. To reduce the risk of multiple servers becoming inaccessible at the same time, they are physically located in different zones of the data center.

The application servers apply auto-scaling to deal with peak times. In the event of a high load, the number of servers is expanded fully automatically in order to reduce the global load to a level that offers an optimal user experience and quick response times.

Analytics

Service usage metrics - Yes

Metrics types -

All the metrics are displayed in four different dashboards. The summary dashboard and the user dashboard are available to all customers. They include data on the usage rate of the platform as well as on the demographics of the users themselves. Standard and Premium customers may also gain access to two deeper data insight features (idea clusters and idea mapping). Both of these are enabled by our in-house built natural language processing (NLP) technology.

Reporting types

- Real-time dashboards
- Regular reports

Resellers

Supplier type - Not a reseller

Staff security

Staff security clearance - Staff screening not performed

Government security clearance - Up to Baseline Personnel Security Standard (BPSS)

Asset protection

Knowledge of data storage and processing locations - Yes

Data storage and processing locations - United Kingdom

- European Economic Area (EEA)
- EU-US Privacy Shield agreement locations

User control over data storage and processing locations - Yes

Datacentre security standards - Complies with a recognised standard (for example CSA CCM version 3.0)

Penetration testing frequency - At least once a year

Penetration testing approach - 'IT Health Check' performed by a CHECK service provider

Protecting data at rest - Physical access control, complying with SSAE-16 / ISAE 3402

Data sanitisation process - Yes

Data sanitisation type - Deleted data can't be directly accessed

Equipment disposal approach - In-house destruction process

Data importing and exporting

Data export approach -

> At any time, all data can be exported by a single click on the button. When using Typeform as survey service within your platform, the survey results become accessible as well. Not only can you link them to the users of your platform, you can also easily export all answers.

Data export formats

- CSV
- Other

Other data export formats - XLSX

Data import formats

- CSV
- Other

Other data import formats - XLSX

Data-in-transit protection

Data protection between buyer and supplier networks - TLS (version 1.2 or above)

Data protection within supplier network - TLS (version 1.2 or above)

Availability and resilience

Guaranteed availability -

> The Services shall be available more than 99%, measured monthly, excluding scheduled maintenance. If Customer requests maintenance during these hours, any uptime or downtime calculation will exclude periods affected by such maintenance. Further, any downtime resulting from outages of third party connections or utilities or other reasons beyond Company's control will also be excluded from any such calculation. Customer's sole and exclusive remedy, and Company's entire liability, in connection with Service availability shall be that for each period of downtime lasting longer than one hour, Company will credit Customer 5% of Service fees for each period of 60 or more consecutive minutes of downtime; provided that no more than one such credit will accrue per day. Downtime shall begin to accrue as soon as Customer (with notice to Company) recognises that downtime is taking place. To receive downtime credit, Customer must notify Company in writing within 24hours from the time of downtime, and failure to provide such notice will forfeit the right to receive downtime credit. Such credits may not be redeemed for cash and shall not be cumulative beyond a total of credits for one (1) week of Service Fees in any one (1) calendar month in any event.

Approach to resilience - This information is available upon request.

Outage reporting - Service outages are reported over email.

Identity and authentication

User authentication needed - Yes

User authentication

- Identity federation with existing provider (for example Google Apps)
- Username or password

Access restrictions in management interfaces and support channels -

> Administrators and project moderators need to authenticate in order to use the management interfaces and support channels. The application layer has a permission system that specifies access policies for every user role and every read/and write action on every data resource. These policies are automatically tested in every change to the application.

Access restriction testing frequency - At least once a year

Management access authentication -

- Identity federation with existing provider (for example Google Apps)
- Username or password

Audit information for users

Access to user activity audit information - Users contact the support team to get audit information

How long user audit data is stored for - Between 6 months and 12 months

Access to supplier activity audit information - Users contact the support team to get audit information

How long supplier audit data is stored for - Between 6 months and 12 months

How long system logs are stored for - Between 6 months and 12 months

Standards and certifications

ISO/IEC 27001 certification - No

ISO 28000:2007 certification - No

CSA STAR certification - No

PCI certification - No

Other security certifications - Yes

Any other security certifications - Cyber Security Essential

Security governance

Named board-level person responsible for service security - Yes

Security governance certified - No

Security governance approach -

> Our information security management system (ISMS) is based on the ISO 27001 specification and describes how we handle documentation, internal audits, continual improvement, and corrective and preventive action.

Information security policies and processes

Access control policy, Information Security Policy, Incident Response Policy and Incident Response Plan.

The access control policy and information security policy are a core part of the onboarding process of new employees and embedded into our company handbook in an accessible language. There are regular training sessions to remind and update employees on relevant changes.

The incident response policy is a core part of the onboarding of the technical support team and the account management team. Regular sessions are organized to provide updates, and adapt the policies where necessary.

Operational security

Configuration and change management standard - Supplier-defined controls

Configuration and change management approach -

> An internal database, part of the technical knowledge base, tracks all services and code repositories used by the platform, including their deployment information, API serving and consumption. All applications are containerized and tracked through a centralized container registry. Security concerns are an explicit part of the specification documents of all new features or changes to existing features.

Vulnerability management type - Supplier-defined controls

Vulnerability management approach -

The application source code is automatically monitored for CVEs using GitHub's vulnerability alerts database in any library dependencies, upgrading them as soon as possible. We release very frequently, about twice per week. Critical issues are released right away. Static code analysis detect known malicious patterns and blocks them from reaching production deployments.

Protective monitoring type - Supplier-defined controls

Protective monitoring approach –

Server and application access is monitored and anomalies trigger notifications to the support team. Platform administrators are in direct contact with our account managers through e-mail, phone and in-platform chat, which are in direct contact with the 2nd line technical team.

Incident management type - Supplier-defined controls

Incident management approach -

Our incident response plan described how to respond to high, medium and low-medium severity incidents, describing the priority and communication actions to take for each category of severity. For issues with critical severity, there's a critical response plan that gets highest priority. Platform administrators are in direct contact with our account managers through e-mail, phone and in-platform chat, which are in direct contact with the 2nd line technical team.

Secure development

Approach to secure software development best practice - Conforms to a recognised standard, but self-assessed

Public sector networks

Connection to public sector networks - No

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier’s Digital Marketplace pricing document) can’t be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

Y[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link;

G-Cloud 12 Customer Benefits Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)

- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection
- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'
2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on its own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly
9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

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 Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity doesn’t apply to the extent that the Supplier breach is due to a Buyer’s instruction.

11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.5.1 rights granted to the Buyer under this Call-Off Contract

11.5.2 Supplier's performance of the Services

11.5.3 use by the Buyer of the Services

11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.6.1 modify the relevant part of the Services without reducing its functionality or performance

11.6.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

11.6.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.7 Clause 11.5 will not apply if the IPR Claim is from:

11.7.2 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.7.3 other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy: https:/www.gov.uk/government/publications/government-security-classifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets: https://www.cpni.gov.uk/protection-sensitive-information-and-assets

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-management-collection

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6.6 buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (Waiver and cumulative remedies)

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer’s written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement
29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29.2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.6.1 its failure to comply with the provisions of this clause

29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 3: Collaboration agreement

This agreement is made on [enter date]

between:

1) [Buyer name] of [Buyer address] (the Buyer)

2) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

3) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

4) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

5) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

6) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address] together (the Collaboration Suppliers and each of them a Collaboration Supplier).

Whereas the:

- Buyer and the Collaboration Suppliers have entered into the Call-Off Contracts (defined below) for the provision of various IT and telecommunications (ICT) services
- Collaboration Suppliers now wish to provide for the ongoing cooperation of the Collaboration Suppliers in the provision of services under their respective Call-Off Contract to the Buyer

In consideration of the mutual covenants contained in the Call-Off Contracts and this Agreement and intending to be legally bound, the parties agree as follows:

1. Definitions and interpretation

1.1 As used in this Agreement, the capitalised expressions will have the following meanings unless the context requires otherwise:

1.1.1 “Agreement” means this collaboration agreement, containing the Clauses and Schedules

1.1.2 “Call-Off Contract” means each contract that is let by the Buyer to one of the Collaboration Suppliers

1.1.3 “Contractor’s Confidential Information” has the meaning set out in the Call-Off Contracts

1.1.4 “Confidential Information” means the Buyer Confidential Information or any Collaboration Supplier's Confidential Information

1.1.5 “Collaboration Activities” means the activities set out in this Agreement

1.1.6 “Buyer Confidential Information” has the meaning set out in the Call-Off Contract

1.1.7 “Default” means any breach of the obligations of any Collaboration Supplier or any Default, act, omission, negligence or statement of any Collaboration Supplier, its employees, servants, agents or subcontractors in connection with or in relation to the subject matter of this Agreement and in respect of which such Collaboration Supplier is liable (by way of indemnity or otherwise) to the other parties

1.1.8 “Detailed Collaboration Plan” has the meaning given in clause 3.2

1.1.9 “Dispute Resolution Process” means the process described in clause 9

1.1.10 “Effective Date” means [insert date]

1.1.11 “Force Majeure Event” has the meaning given in clause 11.1.1

1.1.12 “Mediator” has the meaning given to it in clause 9.3.1

1.1.13 “Outline Collaboration Plan” has the meaning given to it in clause 3.1

1.1.14 “Term” has the meaning given to it in clause 2.1

1.1.15 "Working Day" means any day other than a Saturday, Sunday or public holiday in England and Wales

1.2 General

1.2.1 As used in this Agreement the:

1.2.1.1 masculine includes the feminine and the neuter

1.2.1.2 singular includes the plural and the other way round

1.2.1.3 A reference to any statute, enactment, order, regulation or other similar instrument will be viewed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent re-enactment.

1.2.2 Headings are included in this Agreement for ease of reference only and will not affect the interpretation or construction of this Agreement.

1.2.3 References to Clauses and Schedules are, unless otherwise provided, references to clauses of and schedules to this Agreement.

1.2.4 Except as otherwise expressly provided in this Agreement, all remedies available to any party under this Agreement are cumulative and may be exercised concurrently or separately and the exercise of any one remedy will not exclude the exercise of any other remedy.

1.2.5 The party receiving the benefit of an indemnity under this Agreement will use its reasonable endeavours to mitigate its loss covered by the indemnity.

2. Term of the agreement

2.1 This Agreement will come into force on the Effective Date and, unless earlier terminated in accordance with clause 10, will expire 6 months after the expiry or termination (however arising) of the exit period of the last Call-Off Contract (the “Term”).

2.2 A Collaboration Supplier’s duty to perform the Collaboration Activities will continue until the end of the exit period of its last relevant Call-Off Contract.

3. Provision of the collaboration plan

3.1 The Collaboration Suppliers will, within 2 weeks (or any longer period as notified by the Buyer in writing) of the Effective Date, provide to the Buyer detailed proposals for the Collaboration Activities they require from each other (the “Outline Collaboration Plan”).

3.2 Within 10 Working Days (or any other period as agreed in writing by the Buyer and the Collaboration Suppliers) of [receipt of the proposals] or [the Effective Date], the Buyer will prepare a plan for the Collaboration Activities (the “Detailed Collaboration Plan”). The Detailed Collaboration Plan will include full details of the activities and interfaces that involve all of the Collaboration Suppliers to ensure the receipt of the services under each Collaboration Supplier’s respective [contract] [Call-Off Contract], by the Buyer. The Detailed Collaboration Plan will be based on the Outline Collaboration Plan and will be submitted to the Collaboration Suppliers for approval.

3.3 The Collaboration Suppliers will provide the help the Buyer needs to prepare the Detailed Collaboration Plan.

3.4 The Collaboration Suppliers will, within 10 Working Days of receipt of the Detailed Collaboration Plan, either:

3.4.1 approve the Detailed Collaboration Plan
3.4.2 reject the Detailed Collaboration Plan, giving reasons for the rejection

3.5 The Collaboration Suppliers may reject the Detailed Collaboration Plan under clause 3.4.2 only if it is not consistent with their Outline Collaboration Plan in that it imposes additional, more onerous, obligations on them.

3.6 If the parties fail to agree the Detailed Collaboration Plan under clause 3.4, the dispute will be resolved using the Dispute Resolution Process.

4. Collaboration activities

4.1 The Collaboration Suppliers will perform the Collaboration Activities and all other obligations of this Agreement in accordance with the Detailed Collaboration Plan.

4.2 The Collaboration Suppliers will provide all additional cooperation and assistance as is reasonably required by the Buyer to ensure the continuous delivery of the services under the Call-Off Contract.

4.3 The Collaboration Suppliers will ensure that their respective subcontractors provide all co-operation and assistance as set out in the Detailed Collaboration Plan.

5. Invoicing

5.1 If any sums are due under this Agreement, the Collaboration Supplier responsible for paying the sum will pay within 30 Working Days of receipt of a valid invoice.

5.2 Interest will be payable on any late payments under this Agreement under the Late Payment of Commercial Debts (Interest) Act 1998, as amended.

6. Confidentiality

6.1 Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information, the Collaboration Suppliers acknowledge that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.

6.2 Each Collaboration Supplier warrants that:

6.2.1 any person employed or engaged by it (in connection with this Agreement in the course of such employment or engagement) will only use Confidential Information for the purposes of this Agreement

6.2.2 any person employed or engaged by it (in connection with this Agreement) will not disclose any Confidential Information to any third party without the prior written consent of the other party

6.2.3 it will take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (except as agreed) or used other than for the purposes of this Agreement by its employees, servants, agents or subcontractors

6.2.4 neither it nor any person engaged by it, whether as a servant or a consultant or otherwise, will use the Confidential Information for the solicitation of business from the other or from the other party's servants or consultants or otherwise

6.3 The provisions of clauses 6.1 and 6.2 will not apply to any information which is:

6.3.1 or becomes public knowledge other than by breach of this clause 6

6.3.2 in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party

6.3.3 received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure

6.3.4 independently developed without access to the Confidential Information

6.3.5 required to be disclosed by law or by any judicial, arbitral, regulatory or other authority of competent jurisdiction

6.4 The Buyer’s right, obligations and liabilities in relation to using and disclosing any Collaboration Supplier’s Confidential Information provided under this Agreement and the Collaboration Supplier’s right, obligations and liabilities in relation to using and disclosing any of the Buyer’s Confidential Information provided under this Agreement, will be as set out in the [relevant contract] [Call-Off Contract].

7. Warranties

7.1 Each Collaboration Supplier warrant and represent that:

7.1.1 it has full capacity and authority and all necessary consents (including but not limited to, if its processes require, the consent of its parent company) to enter into and to perform this Agreement and that this Agreement is executed by an authorised representative of the Collaboration Supplier

7.1.2 its obligations will be performed by appropriately experienced, qualified and trained personnel with all due skill, care and diligence including but not limited to good industry practice and (without limiting the generality of this clause 7) in accordance with its own established internal processes

7.2 Except as expressly stated in this Agreement, all warranties and conditions, whether express or implied by statute, common law or otherwise (including but not limited to fitness for purpose) are excluded to the extent permitted by law.

8. Limitation of liability

8.1 None of the parties exclude or limit their liability for death or personal injury resulting from negligence, or for any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.

8.2 Nothing in this Agreement will exclude or limit the liability of any party for fraud or fraudulent misrepresentation.

8.3 Subject always to clauses 8.1 and 8.2, the liability of the Buyer to any Collaboration Suppliers for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement (excluding Clause 6.4, which will be subject to the limitations of liability set out in the relevant Contract) will be limited to [(£,000)].

8.4 Subject always to clauses 8.1 and 8.2, the liability of each Collaboration Supplier for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement will be limited to [Buyer to specify].

8.5 Subject always to clauses 8.1, 8.2 and 8.6 and except in respect of liability under clause 6 (excluding clause 6.4, which will be subject to the limitations of liability set out in the [relevant contract] [Call-Off Contract]), in no event will any party be liable to any other for:

8.5.1 indirect loss or damage
8.5.2 special loss or damage
8.5.3 consequential loss or damage
8.5.4 loss of profits (whether direct or indirect)
8.5.5 loss of turnover (whether direct or indirect)
8.5.6 loss of business opportunities (whether direct or indirect)
8.5.7 damage to goodwill (whether direct or indirect)

8.6 Subject always to clauses 8.1 and 8.2, the provisions of clause 8.5 will not be taken as limiting the right of the Buyer to among other things, recover as a direct loss any:

8.6.1 additional operational or administrative costs and expenses arising from a Collaboration Supplier’s Default

8.6.2 wasted expenditure or charges rendered unnecessary or incurred by the Buyer arising from a Collaboration Supplier's Default

9. Dispute resolution process

9.1 All disputes between any of the parties arising out of or relating to this Agreement will be referred, by any party involved in the dispute, to the representatives of the parties specified in the Detailed Collaboration Plan.

9.2 If the dispute cannot be resolved by the parties' representatives nominated under clause 9.1 within a maximum of 5 Working Days (or any other time agreed in writing by the parties) after it has been referred to them under clause 9.1, then except if a party seeks urgent injunctive relief, the parties will refer it to mediation under the process set out in clause 9.3 unless the Buyer considers (acting reasonably and considering any objections to mediation raised by the other parties) that the dispute is not suitable for resolution by mediation.

9.3 The process for mediation and consequential provisions for mediation are:

9.3.1 a neutral adviser or mediator will be chosen by agreement between the parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one party to the other parties to appoint a Mediator or if the Mediator agreed upon is unable or unwilling to act, any party will within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to the parties that he is unable or unwilling to act, apply to the President of the Law Society to appoint a Mediator

9.3.2 the parties will within 10 Working Days of the appointment of the Mediator meet to agree a programme for the exchange of all relevant information and the structure of the negotiations

9.3.3 unless otherwise agreed by the parties in writing, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the parties in any future proceedings

9.3.4 if the parties reach agreement on the resolution of the dispute, the agreement will be put in writing and will be binding on the parties once it is signed by their authorised representatives

9.3.5 failing agreement, any of the parties may invite the Mediator to provide a non-binding but informative opinion in writing. The opinion will be provided on a without prejudice basis and will not be used in evidence in any proceedings relating to this Agreement without the prior written consent of all the parties

9.3.6 if the parties fail to reach agreement in the structured negotiations within 20 Working Days of the Mediator being appointed, or any longer period the parties agree on, then any dispute or difference between them may be referred to the courts

9.4 The parties must continue to perform their respective obligations under this Agreement and under their respective Contracts pending the resolution of a dispute.

10. Termination and consequences of termination

10.1 Termination

10.1.1 The Buyer has the right to terminate this Agreement at any time by notice in writing to the Collaboration Suppliers whenever the Buyer has the right to terminate a Collaboration Supplier's [respective contract] [Call-Off Contract].

10.1.2 Failure by any of the Collaboration Suppliers to comply with their obligations under this Agreement will constitute a Default under their [relevant contract] [Call-Off Contract]. In this case, the Buyer also has the right to terminate by notice in writing the participation of any Collaboration Supplier to this Agreement and sever its name from the list of Collaboration Suppliers, so that this Agreement will continue to operate between the Buyer and the remaining Collaboration Suppliers.

10.2 Consequences of termination

10.2.1 Subject to any other right or remedy of the parties, the Collaboration Suppliers and the Buyer will continue to comply with their respective obligations under the [contracts] [Call-Off Contracts] following the termination (however arising) of this Agreement.

10.2.2 Except as expressly provided in this Agreement, termination of this Agreement will be without prejudice to any accrued rights and obligations under this Agreement.

11. General provisions

11.1 Force majeure

11.1.1 For the purposes of this Agreement, the expression "Force Majeure Event" will mean any cause affecting the performance by a party of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to any party, the party's personnel or any other failure of a Subcontractor.

11.1.2 Subject to the remaining provisions of this clause 11.1, any party to this Agreement may claim relief from liability for non-performance of its obligations to the extent this is due to a Force Majeure Event.

11.1.3 A party cannot claim relief if the Force Majeure Event or its level of exposure to the event is attributable to its wilful act, neglect or failure to take reasonable precautions against the relevant Force Majeure Event.

11.1.4 The affected party will immediately give the other parties written notice of the Force Majeure Event. The notification will include details of the Force Majeure Event together

with evidence of its effect on the obligations of the affected party, and any action the affected party proposes to take to mitigate its effect.

11.1.5 The affected party will notify the other parties in writing as soon as practicable after the Force Majeure Event ceases or no longer causes the affected party to be unable to comply with its obligations under this Agreement. Following the notification, this Agreement will continue to be performed on the terms existing immediately before the Force Majeure Event unless agreed otherwise in writing by the parties.

11.2 Assignment and subcontracting

11.2.1 Subject to clause 11.2.2, the Collaboration Suppliers will not assign, transfer, novate, sub-license or declare a trust in respect of its rights under all or a part of this Agreement or the benefit or advantage without the prior written consent of the Buyer.

11.2.2 Any subcontractors identified in the Detailed Collaboration Plan can perform those elements identified in the Detailed Collaboration Plan to be performed by the Subcontractors.

11.3 Notices

11.3.1 Any notices given under or in relation to this Agreement will be deemed to have been properly delivered if sent by recorded or registered post or by fax and will be deemed for the purposes of this Agreement to have been given or made at the time the letter would, in the ordinary course of post, be delivered or at the time shown on the sender's fax transmission report.

11.3.2 For the purposes of clause 11.3.1, the address of each of the parties are those in the Detailed Collaboration Plan.

11.4 Entire agreement

11.4.1 This Agreement, together with the documents and agreements referred to in it, constitutes the entire agreement and understanding between the parties in respect of the matters dealt with in it and supersedes any previous agreement between the Parties about this.

11.4.2 Each of the parties agrees that in entering into this Agreement and the documents and agreements referred to in it does not rely on, and will have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement. The only remedy available to each party in respect of any statements, representation, warranty or understanding will be for breach of contract under the terms of this Agreement.

11.4.3 Nothing in this clause 11.4 will exclude any liability for fraud.

11.5 Rights of third parties

Nothing in this Agreement will grant any right or benefit to any person other than the parties or their respective successors in title or assignees, or entitle a third party to enforce any provision and the parties do not intend that any term of this Agreement should be enforceable by a third party by virtue of the Contracts (Rights of Third Parties) Act 1999.

11.6 Severability

If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, that provision will be severed without effect to the remaining provisions. If a provision of this Agreement that is fundamental to the accomplishment of the purpose of this Agreement is held to any extent to be invalid, the parties will immediately commence good faith negotiations to remedy that invalidity.

11.7 Variations

No purported amendment or variation of this Agreement or any provision of this Agreement will be effective unless it is made in writing by the parties.

11.8 No waiver

The failure to exercise, or delay in exercising, a right, power or remedy provided by this Agreement or by law will not constitute a waiver of that right, power or remedy. If a party waives a breach of any provision of this Agreement this will not operate as a waiver of a subsequent breach of that provision, or as a waiver of a breach of any other provision.

11.9 Governing law and jurisdiction

This Agreement will be governed by and construed in accordance with English law and without prejudice to the Dispute Resolution Process, each party agrees to submit to the exclusive jurisdiction of the courts of England and Wales.

Executed and delivered as an agreement by the parties or their duly authorised attorneys the day and year first above written.

For and on behalf of the Buyer

Signed by:

Full name (capitals):
Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position:
Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position:
Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position:
Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position:
Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position:
Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position:

Date:

Collaboration Agreement Schedule 1: List of contracts

Collaboration supplier	**Name/reference of contract**	**Effective date of contract**

Collaboration Agreement Schedule 2 [Insert Outline Collaboration Plan]

Schedule 4: Alternative clauses

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

2.1 The Customer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 8.12 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.2.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Customer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000

- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004
- Work and Families (Northern Ireland) Order 2006

and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

a. persons of different religious beliefs or political opinions
b. men and women or married and unmarried persons
c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
f. persons of different ages
g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

a. the issue of written instructions to staff and other relevant persons
b. the appointment or designation of a senior manager with responsibility for equal opportunities
c. training of all staff and other relevant persons in equal opportunities and harassment matters
d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or

B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Customer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer’s cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee

A Guarantee should only be requested if the Supplier's financial standing is not enough on its own to guarantee delivery of the Services. This is a draft form of guarantee which can be used to procure a Call Off Guarantee, and so it will need to be amended to reflect the Beneficiary's requirements

This deed of guarantee is made on [**insert date, month, year]** between:

(1) [**Insert the name of the Guarantor]** a company incorporated in England and Wales with number [insert company number] whose registered office is at [i**nsert details of the guarantor's registered office**] [or a company incorporated under the Laws of [**insert country**], registered in [**insert country**] with number [**insert number**] at [**insert place of registration**], whose principal office is at [**insert office details**]]('Guarantor'); in favour of

and

(2) The Buyer whose offices are [**insert Buyer's official address**] ('Beneficiary')

Whereas:

(A) The guarantor has agreed, in consideration of the Buyer entering into the Call-Off Contract with the Supplier, to guarantee all of the Supplier's obligations under the Call-Off Contract.

(B) It is the intention of the Parties that this document be executed and take effect as a deed.

[Where a deed of guarantee is required, include the wording below and populate the box below with the guarantor company's details. If a deed of guarantee isn't needed then the section below and other references to the guarantee should be deleted.

Suggested headings are as follows:

- Demands and notices
- Representations and Warranties
- Obligation to enter into a new Contract
- Assignment
- Third Party Rights
- Governing Law
- This Call-Off Contract is conditional upon the provision of a Guarantee to the Buyer from the guarantor in respect of the Supplier.]

Guarantor company	[**Enter Company name**] **'Guarantor'**
Guarantor company address	[**Enter Company address**]
Account manager	[**Enter Account Manager name]**
	Address: [**Enter Account Manager address]**
	Phone: [**Enter Account Manager phone number]**
	Email: [**Enter Account Manager email**]
	Fax: [**Enter Account Manager fax** if applicable]

In consideration of the Buyer entering into the Call-Off Contract, the Guarantor agrees with the Buyer as follows:

Definitions and interpretation

In this Deed of Guarantee, unless defined elsewhere in this Deed of Guarantee or the context requires otherwise, defined terms will have the same meaning as they have for the purposes of the Call-Off Contract.

Term	Meaning
Call-Off Contract	Means [the Guaranteed Agreement] made between the Buyer and the Supplier on [insert date].
Guaranteed Obligations	Means all obligations and liabilities of the Supplier to the Buyer under the Call-Off Contract together with all obligations owed by the Supplier to the Buyer that are supplemental to, incurred under, ancillary to or calculated by reference to the Call-Off Contract.
Guarantee	Means the deed of guarantee described in the Order Form (Parent Company Guarantee).

References to this Deed of Guarantee and any provisions of this Deed of Guarantee or to any other document or agreement (including to the Call-Off Contract) apply now, and as amended, varied, restated, supplemented, substituted or novated in the future.

Unless the context otherwise requires, words importing the singular are to include the plural and vice versa.

References to a person are to be construed to include that person's assignees or transferees or successors in title, whether direct or indirect.

The words ‘other’ and ‘otherwise’ are not to be construed as confining the meaning of any following words to the class of thing previously stated if a wider construction is possible.

Unless the context otherwise requires:

- reference to a gender includes the other gender and the neuter
- references to an Act of Parliament, statutory provision or statutory instrument also apply if amended, extended or re-enacted from time to time

- any phrase introduced by the words ‘including’, ‘includes’, ‘in particular’, ‘for example’ or similar, will be construed as illustrative and without limitation to the generality of the related general words

References to Clauses and Schedules are, unless otherwise provided, references to Clauses of and Schedules to this Deed of Guarantee.

References to liability are to include any liability whether actual, contingent, present or future.

Guarantee and indemnity

The Guarantor irrevocably and unconditionally guarantees that the Supplier duly performs all of the guaranteed obligations due by the Supplier to the Buyer.

If at any time the Supplier will fail to perform any of the guaranteed obligations, the Guarantor irrevocably and unconditionally undertakes to the Buyer it will, at the cost of the Guarantor:

- fully perform or buy performance of the guaranteed obligations to the Buyer

- as a separate and independent obligation and liability, compensate and keep the Buyer compensated against all losses and expenses which may result from a failure by the Supplier to perform the guaranteed obligations under the Call-Off Contract

As a separate and independent obligation and liability, the Guarantor irrevocably and unconditionally undertakes to compensate and keep the Buyer compensated on demand against all losses and expenses of whatever nature, whether arising under statute, contract or at common Law, if any obligation guaranteed by the guarantor is or becomes unenforceable, invalid or illegal as if the obligation guaranteed had not become unenforceable, invalid or illegal provided that the guarantor's liability will be no greater than the Supplier's liability would have been if the obligation guaranteed had not become unenforceable, invalid or illegal.

Obligation to enter into a new contract

If the Call-Off Contract is terminated or if it is disclaimed by a liquidator of the Supplier or the obligations of the Supplier are declared to be void or voidable, the Guarantor will, at the request of the Buyer, enter into a Contract with the Buyer in the same terms as the Call-Off Contract and the obligations of the Guarantor under such substitute agreement will be the same as if the Guarantor had been original obligor under the Call-Off Contract or under an agreement entered into on the same terms and at the same time as the Call-Off Contract with the Buyer.

Demands and notices

Any demand or notice served by the Buyer on the Guarantor under this Deed of Guarantee will be in writing, addressed to:

[**Enter Address of the Guarantor in England and Wales**]

[**Enter Email address of the Guarantor representative**]

For the Attention of [**insert details**]

or such other address in England and Wales as the Guarantor has notified the Buyer in writing as being an address for the receipt of such demands or notices.

Any notice or demand served on the Guarantor or the Buyer under this Deed of Guarantee will be deemed to have been served if:

- delivered by hand, at the time of delivery
- posted, at 10am on the second Working Day after it was put into the post
- sent by email, at the time of despatch, if despatched before 5pm on any Working Day, and in any other case at 10am on the next Working Day

In proving Service of a notice or demand on the Guarantor or the Buyer, it will be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter, or that the fax message was properly addressed and despatched.

Any notice purported to be served on the Buyer under this Deed of Guarantee will only be valid when received in writing by the Buyer.

Beneficiary's protections

The Guarantor will not be discharged or released from this Deed of Guarantee by:

- any arrangement made between the Supplier and the Buyer (whether or not such arrangement is made with the assent of the Guarantor)
- any amendment to or termination of the Call-Off Contract
- any forbearance or indulgence as to payment, time, performance or otherwise granted by the Buyer (whether or not such amendment, termination, forbearance or indulgence is made with the assent of the Guarantor)
- the Buyer doing (or omitting to do) anything which, but for this provision, might exonerate the Guarantor

This Deed of Guarantee will be a continuing security for the Guaranteed Obligations and accordingly:

- it will not be discharged, reduced or otherwise affected by any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations or by any omission or delay on the part of the Buyer in exercising its rights under this Deed of Guarantee

- it will not be affected by any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, control or ownership, insolvency, liquidation, administration, appointment of a receiver, voluntary arrangement, any legal limitation or other incapacity, of the Supplier, the Buyer, the Guarantor or any other person
- if, for any reason, any of the Guaranteed Obligations is void or unenforceable against the Supplier, the Guarantor will be liable for that purported obligation or liability as if the same were fully valid and enforceable and the Guarantor were principal debtor
- the rights of the Buyer against the Guarantor under this Deed of Guarantee are in addition to, will not be affected by and will not prejudice, any other security, guarantee, indemnity or other rights or remedies available to the Buyer

The Buyer will be entitled to exercise its rights and to make demands on the Guarantor under this Deed of Guarantee as often as it wishes. The making of a demand (whether effective, partial or defective) relating to the breach or non-performance by the Supplier of any Guaranteed Obligation will not preclude the Buyer from making a further demand relating to the same or some other Default regarding the same Guaranteed Obligation.

The Buyer will not be obliged before taking steps to enforce this Deed of Guarantee against the Guarantor to:

- obtain judgment against the Supplier or the Guarantor or any third party in any court
- make or file any claim in a bankruptcy or liquidation of the Supplier or any third party
- take any action against the Supplier or the Guarantor or any third party
- resort to any other security or guarantee or other means of payment

No action (or inaction) by the Buyer relating to any such security, guarantee or other means of payment will prejudice or affect the liability of the Guarantor.

The Buyer's rights under this Deed of Guarantee are cumulative and not exclusive of any rights provided by Law. The Buyer’s rights may be exercised as often as the Buyer deems expedient. Any waiver by the Buyer of any terms of this Deed of Guarantee, or of any Guaranteed Obligations, will only be effective if given in writing and then only for the purpose and upon the terms and conditions on which it is given.

Any release, discharge or settlement between the Guarantor and the Buyer will be conditional upon no security, disposition or payment to the Buyer by the Guarantor or any other person being void, set aside or ordered to be refunded following any enactment or Law relating to liquidation, administration or insolvency or for any other reason. If such condition will not be fulfilled, the Buyer will be entitled to enforce this Deed of Guarantee subsequently as if such release, discharge or settlement had not occurred and any such payment had not been made. The Buyer will be entitled to retain this security before and after the payment, discharge or satisfaction of all monies, obligations and liabilities that are or may become due owing or incurred to the Buyer from the Guarantor for such period as the Buyer may determine.

Representations and warranties

The Guarantor hereby represents and warrants to the Buyer that:

- the Guarantor is duly incorporated and is a validly existing company under the Laws of its place of incorporation
- has the capacity to sue or be sued in its own name
- the Guarantor has power to carry on its business as now being conducted and to own its Property and other assets
- the Guarantor has full power and authority to execute, deliver and perform its obligations under this Deed of Guarantee and no limitation on the powers of the Guarantor will be exceeded as a result of the Guarantor entering into this Deed of Guarantee
- the execution and delivery by the Guarantor of this Deed of Guarantee and the performance by the Guarantor of its obligations under this Deed of Guarantee including entry into and performance of a Call-Off Contract following Clause 3) have been duly authorised by all necessary corporate action and do not contravene or conflict with:
    - the Guarantor's memorandum and articles of association or other equivalent constitutional documents, any existing Law, statute, rule or Regulation or any judgment, decree or permit to which the Guarantor is subject
    - the terms of any agreement or other document to which the Guarantor is a party or which is binding upon it or any of its assets
    - all governmental and other authorisations, approvals, licences and consents, required or desirable

This Deed of Guarantee is the legal valid and binding obligation of the Guarantor and is enforceable against the Guarantor in accordance with its terms.

Payments and set-off

All sums payable by the Guarantor under this Deed of Guarantee will be paid without any set-off, lien or counterclaim, deduction or withholding, except for those required by Law. If any deduction or withholding must be made by Law, the Guarantor will pay that additional amount to ensure that the Buyer receives a net amount equal to the full amount which it would have received if the payment had been made without the deduction or withholding.

The Guarantor will pay interest on any amount due under this Deed of Guarantee at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.

The Guarantor will reimburse the Buyer for all legal and other costs (including VAT) incurred by the Buyer in connection with the enforcement of this Deed of Guarantee.

Guarantor’s acknowledgement

The Guarantor warrants, acknowledges and confirms to the Buyer that it has not entered into this Deed of Guarantee in reliance upon the Buyer nor been induced to enter into this Deed of Guarantee

by any representation, warranty or undertaking made by, or on behalf of the Buyer, (whether express or implied and whether following statute or otherwise) which is not in this Deed of Guarantee.

Assignment

The Buyer will be entitled to assign or transfer the benefit of this Deed of Guarantee at any time to any person without the consent of the Guarantor being required and any such assignment or transfer will not release the Guarantor from its liability under this Guarantee.

The Guarantor may not assign or transfer any of its rights or obligations under this Deed of Guarantee.

Severance

If any provision of this Deed of Guarantee is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision will be severed and the remainder of the provisions will continue in full force and effect as if this Deed of Guarantee had been executed with the invalid, illegal or unenforceable provision eliminated.

Third-party rights

A person who is not a Party to this Deed of Guarantee will have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Deed of Guarantee. This Clause does not affect any right or remedy of any person which exists or is available otherwise than following that Act.

Governing law

This Deed of Guarantee, and any non-Contractual obligations arising out of or in connection with it, will be governed by and construed in accordance with English Law.

The Guarantor irrevocably agrees for the benefit of the Buyer that the courts of England will have jurisdiction to hear and determine any suit, action or proceedings and to settle any dispute which may arise out of or in connection with this Deed of Guarantee and for such purposes hereby irrevocably submits to the jurisdiction of such courts.

Nothing contained in this Clause will limit the rights of the Buyer to take proceedings against the Guarantor in any other court of competent jurisdiction, nor will the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable Law).

The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.

[The Guarantor hereby irrevocably designates, appoints and empowers [**enter the Supplier name**] [or a suitable alternative to be agreed if the Supplier's registered office is not in England or Wales] either at its registered office or on fax number [**insert fax number**] from time to time to act as its authorised agent to receive notices, demands, Service of process and any other legal summons in England and Wales for the purposes of any legal action or proceeding brought or to be brought by the Buyer in respect of this Deed of Guarantee. The Guarantor hereby irrevocably consents to the Service of notices and demands, Service of process or any other legal summons served in such way.]

IN WITNESS whereof the Guarantor has caused this instrument to be executed and delivered as a Deed the day and year first before written.

EXECUTED as a DEED by

[**Insert name of the Guarantor**] acting by [**Insert names**]

Director

Director/Secretary

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes • created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.

Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.

Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)

DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.

G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.

Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium
Intellectual Property Rights or IPR	Intellectual Property Rights are: • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as ‘Intermediaries legislation’. It’s a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.

Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.

Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:
	• induce that person to perform improperly a relevant function or activity
	• reward that person for improper performance of a relevant function or activity
	• commit any offence:
	  ○ under the Bribery Act 2010
	  ○ under legislation creating offences concerning Fraud
	  ○ at common Law concerning Fraud
	  ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation 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.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.

Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.

Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

Annex 1: Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer's Data Protection Officer are: Nimali de Silva, Care Quality Commission, 2 Redman Place 2nd Floor, London E20 1JQ

1.2 The contact details of the Supplier's Data Protection Officer are: Koen Gremmelprez, Citizen Lab, Meusegamsraat 105, 1861 Wolvertem, Belgium.

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Descriptions	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: ● **Digital engagement platform with CQC's stakeholders (public and providers)**
Duration of the Processing	Until 31st October 2023 and any applicable extension period.
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: employment Processing, statutory obligation, recruitment assessment etc]
Type of Personal Data	Name, Email Group or profession represented, The sector they use or work in Regional area(s), Year of birth Gender Ethnic group Sexuality Disability Caring responsibilities Long term conditions If they have used a health/care service in the last 6 months Religion
Categories of Data Subject	Members of the public Health and care staff Individuals responding on behalf of providers Individuals responding on behalf of organisations that represent the public
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	CQC can download all data and remove it from the Citizen Lab platform once the contract ends.

Annex 2: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 4 of the Framework Agreement (Where one Party is Controller and the other Party is Processor) and paragraphs 17-27 of Schedule 4 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [**delete as appropriate Supplier/Buyer**]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [**Supplier's/Buyer's**] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a data subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Buyer each undertake that they shall:

(a) report to the other Party every **[enter number]** months on:

(i) the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses

2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its personnel who have access to the Personal Data and ensure that its personnel:

(i) are aware of and comply with their 's duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach;

and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

(a) the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to the each other 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

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the contract, in accordance with the terms of Article 30 GDPR.

6. ICO Guidance

6.1 The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant central government body. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant central government body.

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("Financial Penalties") then the following shall occur:

(a) if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier’s sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clauses 8.66 to 8.79 of the Framework terms (Managing disputes).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction (“Court”) by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the Court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the “Claim Losses”):

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Not used

9. Termination

9.1 If the Supplier is in material Default under any of its obligations under this Annex 2 (joint controller agreement), the Buyer shall be entitled to terminate the contract by issuing a termination notice to the Supplier in accordance with Clause 18.5 (Ending the contract).

10. Sub-Processing

10.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

11. Data Retention

11.1 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Schedule 8: Supplier Terms

citizenlab

Quote

Annex I: Pricing plans and implementation

Strategy | **Preparation** | **Launch**

	ESSENTIAL	STANDARD	PREMIUM
	Up to 2 admins	**Up to 4 admins**	**Up to 8 admins**
	No project managers	✓Up to 5 project managers	✓Unlimited project managers
✓	Up to 3 active projects	✓Unlimited active projects	✓Unlimited active projects
	No project folders	✓Unlimited project folders	✓Unlimited project folders
✓	**All participation methods** *ideation, mops, survey, poll, PB. proposals*	**All Essential features +**	**All Standard features +**
✓	Customisable design	✓Online workshops	Premium styling options
✓	Communications: emails & widgets	✓Personalised domain	Premium content sections
✓	Manual groups & closed projects	Custom topics, user fields & maps	Integrations & API access
✓	Dashboard & analytics	Smart groups & granular permissions	ID verification & Single Sign-On
		Project reports	AI-assisted data insights
		All Essential services +	**All Standard services +**
	Essential onboarding	✓Standard onboarding	Premium onboarding
	No project design workshops	✓lip to 1 project design workshop	tip to 2 project design workshops
	Participation expert access	Project templates	Priority support

	Platform delivery		Platform build			Platform launch	
Essential	●		●				
Standard	●	●	●	●			●
Premium	●	●	●	●	●	●	●
	Kick-off meeting	Participation strategy workshop				Training session: platform use	Evaluation session
	Training session: platform build			Project design workshop(s)	Platform quality & accessibility review		

Annex II: General Terms and Conditions

1. Definitions

1.1 In these General Terms and Conditions, the below capitalized terms have the following meaning:

"Agreement": this Agreement consists of the accepted Offer, the General Terms and Conditions and its exhibits.

"CitizenLab": CitizenLab NV, having its registered office and principal place of business at 1000 Brussels, Boulevard Anspach 65, Belgium, registered with the Belgian Crossroads Bank for Enterprises under company number 0638.901.287.

"Customer": the (future) contracting party of CitizenLab in respect of whom the Agreement is entered.

"Customer Data": any data that is generated through user input or uploaded by Care Quality Commission through the Services, as well as any data based on or derived thereof or provided to Care Quality Commission as part of the Services.

"Confidential Information: all information that is considered confidential by the parties, either because the parties have clearly identified such information as confidential or proprietary, or because the information should reasonably be considered as confidential in view of the nature of the information or the circumstances. Confidential Information includes, but is not limited to, the terms of this Agreement, trade secrets, user data, and information not generally known to the public, such as business plans, strategies, practices, products, personnel and finance.

"Disclosing Party" means the party that discloses Confidential Information to the Receiving Party under the Agreement.

"Data Processing Agreement": the agreement as attached to this Agreement under Annex II.4. "Equipment": all devices and peripherals necessary to connect, access or otherwise make use of the Services, such as, but not limited to: modems, hardware, servers, software, operating systems networks, and web servers.

"Expiration Date": the date on which the Agreement is terminated.

"Fees": the amounts payable by Care Quality Commission for the use of the Services and for the implementation of the Services.

"Force Majeure": any event or circumstance which is beyond the reasonable control and without the fault of the party affected, and which temporarily or permanently prevents the affected party from (further) performing its contractual obligations under the Agreement. Such events or circumstances are for example, without limitation: riots, wars, acts of terrorism; earthquakes, floods, fires and other natural disasters; sabotages; strikes; epidemics of pandemics; interruptions and malfunctions of computer facilities;

"General Terms and Conditions": these general terms and conditions, including its exhibits, which apply to every Offer made by CitizenLab, every acceptance by Care Quality Commission of an Offer, and in general to every agreement entered within that framework between CitizenLab and Care Quality Commission.

"Intellectual Property Rights": all acquired and future intellectual property rights, including but not limited to copyrights, trademarks, design rights, patents, know-how, trade secrets, inventions, all applications for the protection or registration of these rights and all renewals and extensions thereof existing in any part of the world and all other intellectual property rights protected by any applicable law.

"License": the right of Care Quality Commission conferred by CitizenLab to use the Services in accordance with the Agreement.

"License Commencement Date": the date upon which the License commences, as determined in the accepted Offer.

"License Expiration": the date upon which the License expires, as determined in the accepted Offer.

"License Fee": the portion of the Fee which is paid by Care Quality Commission for the use of the Services.

"Maintenance Window": the time gap between 12 AM (midnight) and 6 AM CET from Mondays to Saturdays, and the entire day on Sundays and Official Belgian holidays.

"Offer": the explicit, written proposal from CitizenLab to Care Quality Commission to enter an agreement.

"Partner": any party who has a contractual relationship with Citizenlab and who acts on behalf of CitizenLab with respect to one or more Services.

"Pricing Plan": the chosen set of Services (Essential, Standard, Premium), as further detailed under Annex I.

"Priority Support": the level of support provided by CitizenLab to a Customer if Care Quality

Commissionopted in for a Premium Pricing Plan, of which the Service Level Objectives are detailed in the Service Level Agreement.

“Privacy Policy”: the current statement of CitizenLab regarding the processing of personal data, as further detailed under Annex II.3

“Receiving Party" means the party receiving Confidential Information from the Disclosing Party under the Agreement.

“Services": the services provided by CitizenLab to Care Quality Commission under this Agreement, including software (platform), know-how, as well as related improvements, extensions and modifications, that will be available and detailed in the applicable Pricing Plan.

“Service Availability:” the time duration during which the Services are available, as measured in minutes over the course of a one-month period, hereby excluding minutes of a Maintenance Window and the minutes dedicated to emergency maintenance.

"Service Credits": an amount to which Care Quality Commission is entitled if a Service Level Objective is not met by CitizenLab, of which the calculation and conditions are set forth in the Service Level Agreement.

“Service Issues”: any interference of the Services as further detailed in the Service Level Agreement.

"Service Level Agreement": the Annex II.2.A <OR> Annex.II.2.B as attached to these General Terms and Conditions.

"Service Level Objectives": the intended levels of the provision of the Services as described in the Service Level Agreement.

“Support”: the support provided by CitizenLab to Care Quality Commission in the context of the Agreement, of which the Service Level Objectives are detailed in the Service Level Agreement.

“Target Resolution Time”: under the condition that Care Quality Commission has opted in for a Premium Pricing Plan, the time gap between the notification of a Service Issue and the temporary or definitive resolution of the Service Issue. The Target Resolution Time is calculated within Working Days and is further specified in the Service Level Agreement.

“Target Response Time”: under the condition that Care Quality Commission has opted in for a Premium Pricing Plan, the time gap between the notification of a Service Issue and the oral or written

acknowledgement by CitizenLab of the Server Issue. The Target Response Time is calculated within Working Days and is further specified in the Service Level Agreement.

"Term": the current or renewed periods during which the Agreement is effective.

"User": any individual end user of the Services who is granted user access to the Services by Care Quality Commission.

"Working Day": Monday to Friday during the hours of 9:00 AM through 6:00 PM Central European Time (CET), with the exclusion of Official Belgian Holidays.

2. Conclusion of the Agreement

2.1 Every Offer is without obligation until the moment of acceptance by Care Quality Commission. By such acceptance, an Agreement is deemed to have been fully and legally entered. The written or electronic signature of the Offer by both parties shall constitute such acceptance.

2.2 By virtue of entering this Agreement, Care Quality Commission shall be assumed to accept these General Terms and Conditions and therefore completely waive the application of its own terms and conditions.

3. Delivery of the Services

3.1 CitizenLab shall make available the Services to Care Quality Commission from the License Commencement Date, in accordance with the Service Level Agreement and the other provisions of the Agreement. Care Quality Commission shall have the right to use the Services within the restrictions set out in the Agreement.

3.2 Subject to the terms hereof, CitizenLab shall provide Care Quality Commission with reasonable technical support services in accordance with the terms set forth in the Service Level Agreement.

3.3 CitizenLab has the right to deliver the implementation and/or general support aspect of the Services by its Partner(s).

3.4 Care Quality Commission may at all times request CitizenLab to upgrade/downgrade to a different Pricing Plan. Such requests shall be delivered in writing or by email. Such a change to a Pricing Plan shall take effect upon acceptance in writing or by email by CitizenLab, which shall be no later than fourteen (14) days following the request of Care Quality Commission.

3.5 If CitizenLab is prevented by Force Majeure of a permanent or temporary nature from performing or further performing the Agreement, regardless of whether the Force Majeure was foreseeable, CitizenLab shall be entitled, without any obligation to pay damages, to terminate the Agreement in whole or in part by means of a written notice without judicial intervention, without prejudice to CitizenLab's right to payment by Care Quality Commission for performance already performed by CitizenLab before there was a situation of Force Majeure or to suspend performance or further performance of the Agreement in whole or in part.

4. Service levels

4.1 CitizenLab commits itself by means of a best-effort obligation to provide the Services in accordance with the Service Level Objectives as determined in the Service Level Agreement.

4.2 If CitizenLab fails to meet the Service Level Objectives, Care Quality Commission is entitled to Service Credits, the calculation of which is included in the Service Level Agreement.

4.3 To the extent reasonably possible, CitizenLab will inform Care Quality Commission of any anticipated failure to meet a Service Level Objective and of the steps CitizenLab shall take (or has already taken), in order to avoid the failure to meet the Service Level Objective, in accordance with the Service Level Agreement.

5. Restrictions and responsibilities

5.1 Care Quality Commission warrants and represents that it shall not, to the extent permissible by mandatory law, when using the Services:

- Reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Services or any software, documentation or data related to the Services.
- Modify, translate, create, or publish derivative works of the Services.
- Remove or obfuscate proprietary notices or labels of CitizenLab or third party proprietaries.
- Otherwise violate the Intellectual Property Rights of CitizenLab or third parties.Care Quality Commission also warrants and represents that it shall undertake its best efforts to promptly remove from the Services any content uploaded by the Users that violates or may violate Intellectual Property Rights of any third party.
- Use the Services for time sharing or service bureau purposes or otherwise for the benefit of a third party.
- Upload malware, viruses, trojan horses, spyware or other similar malicious software.
- Upload and distribute illegal content and content that incites hatred, violence, discrimination or other illegal activities. Care Quality Commission also warrants and represents that it shall

undertake its best efforts to promptly make available any content uploaded by the Users that violates or may the aforementioned cases.

- Use the Services for the purpose of distributing unsolicited electronic communications.
- Interfere, circumvent, or undertake any attempt thereof, with respect to the security features of the Services.
- Undertake any other act that may interfere with the functionality, availability, or integrity of the Services.
- Use the Services in any other way that violates other policies or instructions provided by CitizenLab. It shall be at the discretion of CitizenLab to implement or modify any policy or instruction.
- Use the Services in any other way that violates applicable regulations.

5.2 Furthermore, Care Quality Commission warrants and represents that it shall, while using the Services:

- Promptly obtain the consent of any owner of Intellectual Property Rights to use their works on the Services. Such consent must be promptly obtained as well if a User distributes any aforementioned work. If such consent is not obtained within a reasonable term, or if any content distributed on the Services otherwise infringes the previous paragraph, Care Quality Commission represents and warrants that it shall promptly remove or make unavailable such content without undue delay.
- Obtain, maintain and secure the Equipment, which is the sole responsibility of Care Quality Commission and which does not directly nor indirectly form part of the Services.
- Adopt secure IDs and passwords, and implement appropriate organisational measures with respect to passwords in relation to the access to the Services in line with any possible instructions provided by CitizenLab.
- Inform all Users of the Services (employees, officers, consultants) of these General Terms and Conditions.

5.3 If Care Quality Commission violates any provision of the previous paragraphs, CitizenLab shall have the right to suspend Care Quality Commission's access to the Services, subject to a written notification, either by post letter or by e-mail, two (2) working days in advance. Care Quality Commission shall thereby be requested to inform CitizenLab by written notification, either by post letter or by e-mail, of a potential solution. Upon acceptance by CitizenLab, Care Quality Commission shall remedy the violation within a reasonable time but no later than ten (10) Working Days. In case Care Quality Commission does not remedy this violation within the aforementioned period, CitizenLab has the right (i) to remove the infringing content itself and (ii) to immediately terminate the access to the Services by Care Quality Commission and consider the Agreement as terminated in accordance with article 9, without prejudice to the right of CitizenLab to fully recover any damages from Care Quality Commission.

6. Confidentiality

6.1 The parties accept the disclosure of Confidential Information among themselves. The Receiving Party shall treat and retain such Confidential Information with at least the same care as the Receiving Party undertakes to preserve and secure its own Confidential Information, but in no event shall the Receiving Party treat such information with less than a reasonable degree of care.

6.2 The Receiving Party agrees not to disclose the Confidential Information to anyone other than the employees, affiliates and suppliers of the Receiving Party on a need-to-know basis, always provided that such employees, affiliates or suppliers are aware of the confidential or proprietary nature of the Confidential Information and are subject to confidentiality obligations equivalent to those set out in this Agreement.

6.3 The Receiving Party agrees: (i) to take reasonable precautions to protect such Confidential Information, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third party any such Confidential Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information after five (5) years following the termination of the Agreement or any information of which the Receiving Party can prove (a) it is generally available to the public, or (b) was in its possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Confidential Information of the Disclosing Party or (e) is required to be disclosed by law or pursuant to a court order.

7. Intellectual property

7.1 The parties acknowledge that all Intellectual Property Rights belonging to a party prior to the execution of the Agreement shall remain vested in that party, regardless of the execution of the Agreement.

7.2 Care Quality Commission shall own, or shall have the legitimate right of disposal, in all Intellectual Property Rights on the Customer Data. CitizenLab shall own, or shall have the legitimate right of disposal, in all Intellectual Property Rights in connection to the Services. Nothing in this Agreement shall operate so as to transfer or assign any such Intellectual Property Rights to another party to the Agreement.

7.3 Care Quality Commission is hereby granted a non-exclusive, non-transferable, non-sublicensable License to use the Services subject to the Agreement and within the geographic territory of Care Quality Commission.

7.4 Notwithstanding anything to the contrary, CitizenLab shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the Services and related systems and technologies (including, without limitation, the Customer Data), and CitizenLab shall be entitled (during and after the Term hereof) to (i) use such information and the Customer Data to improve and enhance the Services and for other development, diagnostic and corrective purposes in connection with the Services and other CitizenLab offerings, and (ii) disclose such information and the

Customer Data solely in aggregate or other anonymized form in connection with its business. Such aggregation or anonymisation shall not be undertaken if the Customer Data is processed in accordance with an explicitly identified processing purpose in CitizenLab's Privacy Policy.

8. Pricing and payment of Fees

8.1 All prices quoted are exclusive of VAT and any other taxes, costs, royalties, etc.

8.2 As consideration for the Services, CitizenLab shall invoice the Services by means of a one-off invoice for the total amount as agreed upon. Parties may derogate from the foregoing by agreeing to a yearly instalment payment schedule, in case the Term stretches over multiple years. Implementation fees, custom developments, and other services may be billed separately.

8.3 Payments shall be made in the currency stated on the invoice, with no reductions applied due to taxes (e.g. value-added tax), charges (e.g. bank charges), or any similar fees, whether fiscal or parafiscal, direct or indirect.

8.4 Any request by Care Quality Commission for the development of additional developments by CitizenLab, shall be charged at a 250 EUR/hour fee. Acceptance of the request by CitizenLab, as well as upfront approval from by Customer on the development estimation, are required before any such developments shall be executed.

8.5 Where Care Quality Commission chooses another Pricing Plan in accordance with article 3.4, the following shall apply:

- If such change constitutes an upgrade from Essential to Standard or Premium, or from Standard to Premium, Care Quality Commission shall receive an additional invoice for the prorated amount.
- If such change constitutes a downgrade from Premium to Standard or Essential, or from Standard to Essential, Care Quality Commission shall be entitled to a prorated credit, which will be applied as a reduction on the next invoice (unless Care Quality Commission would not renew the contract, in which case Care Quality Commission gets refunded for the credit amount within 30 days after the termination of the Agreement).
- To illustrate the credit mechanism with an example, if Care Quality Commission has paid a Standard annual License Fee for X and decides to downgrade to Essential, priced at 0.5X, for 4 months to go in the Term, they will receive following credit on their next invoice: (4/12 months) x (X - 0.5X). Assuming Care Quality Commission renews their Agreement with an equal Term of one year, they will pay

8.6 Care Quality Commission shall pay all amounts due in accordance with the Agreement within thirty (30) days after the invoice date. If Care Quality Commission fails to make payment within the aforementioned time frame:

- CitizenLab shall be entitled to late payment compensation of 8% of the amount due (with a minimum of 150 EUR), plus a conventional late payment interest on the overdue amount, equal to the product of (a) 9% on the due amount and (b) the number of days in which payment remains due, divided by 365.
- CitizenLab shall be entitled to suspend the further provision of the Services after ninety (90) days following the payment due date. In that case CitizenLab shall notify Care Quality Commission of the suspension and CitizenLab shall only continue its obligations if Care Quality Commission provides sufficient security for the fulfilment of its obligations.

8.7 Late payment of an invoice causes all outstanding invoices of Care Quality Commission to become due, even if the due date of these invoices has not yet expired.

8.8 CitizenLab reserves the right, at the end of each Term of the Agreement, to formulate the renewal of the Agreement under the resolutive condition of acceptance by Care Quality Commission of modified terms and Fees. CitizenLab shall notify Care Quality Commission of a proposal for an amended Fee at least thirty (30) days prior to the Expiration Date of the current Term of the Agreement. Care Quality Commission shall:

- Either notify CitizenLab in writing of its agreement to the modified terms and/or Fees no later than on the Expiration Date of the Agreement. The lack of such notification shall result in the automatic renewal of the Agreement at modified terms and/or Fees for an equal Term, which commences the day after the Expiration Date.
- Either confirm its disagreement, which shall result in the termination of the Agreement after its Expiration Date.

9. Term and termination

9.1 The Agreement is entered into for the Term specified in the Agreement. No later than thirty (30) days prior to the Expiration Date of the current Term of the Agreement, one party shall notify the other per email or letter if it wishes to terminate the Agreement upon its Expiration Date. In the absence of such notification, the Agreement shall be automatically renewed for an equal and successive Term which commence the day after the Expiration Date.

9.2 Care Quality Commission acknowledges that the following circumstances shall by operation of law give rise to termination of the Agreement within the meaning of this article unless CitizenLab waives this termination in writing and pursues the performance of the Agreement to which CitizenLab is entitled:

- Insolvency of Care Quality Commission, such as bankruptcy.
- Any material breach of articles 5-7.

- Any other material breach of the provisions of the Agreement which Care Quality Commission fails to remedy within fifteen (15) days of Care Quality Commission being notified in writing of the breach by CitizenLab, such as, but not limited to, the non-payment of any pursuant to the Agreement within the agreed payment term. The aforementioned period of fifteen (15) days does not apply if the infringement by Care Quality Commission constitutes a criminal offence, or if the infringement compromises the functionality, availability or integrity of the Services.

9.3 In the event of termination of the Agreement:

- CitizenLab shall make available all the Customer Data to Care Quality Commission for electronic retrieval for a period of ninety (90) days. Thereafter CitizenLab shall retain the Customer Data only for the term referred to in the Data Processing Agreement, after which CitizenLab shall either anonymize the Customer Data or remove it from all its systems. Such removal shall be confirmed in writing by CitizenLab upon request of Care Quality Commission.
- Care Quality Commission shall be encouraged and permitted to export, on an unrestricted basis, any and all user-generated data (incl. ideas, comments, proposals and user lists) via self-service means before the actual Expiration Date of the Agreement.
- Upon the Expiration Date of the Agreement, Care Quality Commission shall lose all administrator and moderation rights and shall be revoked access to the back-office of the Services.
- Without prejudice to article 8.5 and to the Service Level Agreement, no refunds of the amounts paid shall be granted to Care Quality Commission.

9.4 All sections of this Agreement which by their nature should survive termination, shall survive termination, including, without limitation, accrued rights to payment, confidentiality obligations, warranty disclaimers, and limitations of liability.

10. Warranty and liability

10.1 CitizenLab represents and warrants that:

- The Services shall be performed with reasonable skill and care in a timely and professional manner, using appropriately qualified and experienced personnel and in accordance with good industry practice. HOWEVER, CITIZENLAB DOES NOT WARRANT THAT THE SERVICES SHALL BE UNINTERRUPTED OR ERROR-FREE, NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THE AGREEMENT, THE SERVICES ARE PROVIDED "AS IS" AND CITIZENLAB DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
- It shall use its reasonable efforts to ensure that the Services are free from all viruses and other contaminants including any codes or instruction that may be used to access, modify, delete or damage any data files, or other computer programs used by Care Quality Commission, and that for

this purpose, CitizenLab warrants and represents that it shall use the most comprehensive and up to date available virus checker.

- This Agreement is executed by a duly authorized representative of CitizenLab.

10.2 Care Quality Commission represents and warrants that:

- It owns or has obtained valid licenses of all Intellectual Property Rights in relation to the Customer Data uploaded on the Services.
- It owns a valid License for the Services with a clear mention of the License Commencement Date and License Expiration.
- It shall only use the Services in accordance with the terms of the Agreement.
- It shall not undertake any actions or participate in any conduct, even unrelated to the Services, which is intended, or could reasonably be expected, to harm CitizenLab, its reputation or its goodwill, or which could reasonably be expected to lead to unwanted or unfavorable publicity to CitizenLab.
- This Agreement is executed by a duly authorized representative of Care Quality Commission.

10.3 NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXCEPT FOR BODILY INJURY OF A PERSON, CITIZENLAB, ITS PARTNERS, SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL EQUIPMENT AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY:

- FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES.
- FOR ANY EVENT OF FORCE MAJEURE.
- FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED EITHER (1) THE FEES PAID BY [DEAL.COMPANY.NAME] TO CITIZENLAB FOR THE SERVICES IN THE 12 MONTHS PRIOR TO THE ACT THAT GAVE RISE TO THE LIABILITY, WHETHER OR NOT CITIZENLAB HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR (2) THE AMOUNT FOR WHICH THE LIABILITY OF CITIZENLAB IS INSURED.

11. Indemnity

11.1 Care Quality Commission agrees to defend, indemnify and hold harmless CitizenLab, its officers, employees, agents, subsidiaries, affiliates and other partners, from and against any claims, actions or demands, liabilities and settlements including without limitation, reasonable legal and accounting fees, resulting from, or alleged to result from any conduct or misuse of the Services which infringes a provision of articles 5 to 7 (for example, the infringement of any Intellectual Property Right of a third party).

11.2 CitizenLab shall hold Care Quality Commission harmless from liability to third parties resulting from the infringement of CitizenLab of the Agreement, provided CitizenLab is promptly notified of any and all

threats, claims and proceedings related thereto and given reasonable assistance and the opportunity to assume sole control over defense and settlement. CitizenLab shall not be held to indemnification of Care Quality Commission for any settlement for which CitizenLab has not provided prior approval in writing.

11.3 The foregoing obligations do not apply with respect to portions or components of the Services:

- Not supplied by CitizenLab.
- Made in whole or in part in accordance with Customer's specifications.
- Modified after delivery by CitizenLab.
- Combined with other products, processes or materials where the alleged infringement relates to such combination.
- Where Care Quality Commission continues to conduct infringing activities after being notified thereof or after being informed of modifications that would have avoided the alleged infringement.
- Where Care Quality Commission's use of the Service is not strictly in accordance with this Agreement.

11.4 If, due to a claim of infringement, the Services are held by a court of competent jurisdiction to be or are believed by CitizenLab to be infringing, CitizenLab may, at its option and expense:

- replace or modify the Service to be non-infringing provided that such modification or replacement contains substantially similar features and functionality, or;
- obtain for Care Quality Commission a license to continue using the Service, or;
- if neither of the foregoing is commercially workable, terminate this Agreement in accordance with article 9.

12. Miscellaneous

12.1 If any provision of this Agreement is found to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable.

12.2 This Agreement is not assignable, transferable or sublicensable by Care Quality Commission except with CitizenLab's prior written consent. CitizenLab may transfer and assign any of its rights and obligations under this Agreement without consent of Care Quality Commission. CitizenLab shall inform Care Quality Commission in writing in case of any such transfer or assignment.

12.3 This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both parties, except as otherwise provided herein.

12.4 No agency, partnership, joint venture, or employment is created as a result of this Agreement and Care Quality Commission does not have any authority of any kind to bind CitizenLab in any respect whatsoever. In any action or proceeding to enforce rights under this Agreement, the prevailing party shall be entitled to recover costs and attorneys' fees.

12.5 All notices under this Agreement shall be in writing or by e-mail and shall be deemed to have been duly given:

- When receipt is electronically confirmed, if transmitted by facsimile or e-mail.
- The day after it is sent by post letter.
- The date of confirmation of receipt, if sent by certified or registered mail.

12.6 Where Care Quality Commission is located in the United States, this Agreement shall be governed by the Delaware law without regard to its conflict of laws provisions. All claims arising out of or relating to this Agreement shall be exclusively litigated in the courts which hold jurisdiction over the head offices of CitizenLab.

Annex II.2.A: Service Level Agreement (Essential and Standard)

1. Service Level Objectives

1.1 This Service Level Agreement shall provide the Service Level Objective. The provisions of the Service Level Agreement shall prevail the General Terms and Conditions. However, any specific terms in the accepted Offer shall prevail above the Service Level Agreement.

1.2 CitizenLab shall, during the Term of the Agreement, ensure the Service Level Objective of a Service Availability of 99.9%, measured monthly. Downtime shall begin to accrue as soon as Care Quality Commission gives written notice to CitizenLab that downtime is taking place, accompanied by any sort of evidence of the downtime, and continues until the availability of the Services is restored.

1.3 In the event where CitizenLab fails to meet the Service Level Objective, Care Quality Commission shall be entitled, upon its written request, to the following Service Credits, which shall be compensated on the first month following such event:

- Service Availability <99%: reimbursement of 10% of the License Fee, prorated over a one-month period.
- Service Availability <99.5%: reimbursement of 5% of the License Fee, prorated over a one-month period.
- Service Availability <99.9%: reimbursement of 1% of the License Fee, prorated over a one-month

period.

1.4 If and insofar the Service Level was not reached due to Force Majeure, the previous paragraph shall not apply.

1.5 The cumulative amount of Service Credits for a one-month period, shall not exceed the total Fee prorated over a one-week period, nor the amount for which CitizenLab's liability has been insured.

1.6 The Service Credits shall be applied to the portion of the Fee that was paid in the month in which the Service Level Objective was not met.

2. Support hours and contact information

2.1 CitizenLab shall provide Support to Care Quality Commission per email (support@citizenlab.co) or by responding to helpdesk tickets via the CitizenLab platform on Working Days.

Annex II.2.B: Service Level Agreement (Premium)

1. Service Level Objectives

1.1 This Service Level Agreement shall provide the Service Level Objectives. The provisions of the Service Level Agreement shall prevail the General Terms and Conditions. However, any specific terms in the accepted Offer shall prevail above the Service Level Agreement.

1.2 CitizenLab shall, during the Term of the Agreement, ensure the following Service Level Objectives:

1.2.1 CitizenLab ensures a Service Availability of 99.9%, measured monthly. Downtime shall begin to accrue as soon as Care Quality Commission gives written notice to CitizenLab that downtime is taking place, accompanied by any sort of evidence of the downtime, and continues until the availability of the Services is restored.

1.2.2 CitizenLab shall handle Service Issues via the following Priority Support Services:

Definitions of Priority Levels	
Priority Level	*Description*

Critical (Level 1)	The Services, or a critical function, is not functioning properly or integrally unavailable, causing significant impact to Care Quality Commission's operations. Errors that cause data to be lost. No work-around acceptable to Care Quality Commission is available. Examples could include: - Availability of Workshops or one of its critical functions; - Critical project (folder) functionalities for live projects; - Loss of critical data, such as registration and project data; - Systemic login, invitation, or registration issues (encountered by +10% of all users).
Major (Level 2)	One or more non-critical functionalities of the Services are unavailable or present major issues, causing significant impact to Care Quality Commission's operations. An acceptable and temporary work-around is available to Care Quality Commission. Examples could include: - Inability to save changes to a project (folder), or edit pages; - Inability to perform data exports; - Email campaign does not send out; - Inability to add new input by admins or users; - Severe loading speed issues (>5s loading time); - Problems with entering feedback and updating statuses.

Minor (Level 3)	The Services are available, but one or more of its functionalities present issues that have little to no impact on the work of Care Quality Commission. Operations could be improved by correction of a minor error. Examples could include: - Problems embedding a survey; - Support service task requests; - Other unusual invitation, login, and registration issues.
Minimal (Level 4)	Care Quality Commission requires information or assistance about the Services, such as questions about capabilities, installation, configuration, operation, cosmetic, ... Examples could include: - Setting up user verification; - Changes to privacy policy, terms and conditions, etc.; - Adding custom registration data; - Product feedback and feature requests; - Changing color, header, logo, image, copy, language settings.

Error Response and Resolution Commitments		
Priority Level	Targeted Response Time	Targeted Resolution Time
Level 1	9 hours	2 Business Days
Level 2	1 Business Day	4 Business Days
Level 3	2 Business Days	10 Business Days or next software release

Level 4	5 Business Days	Undefined

The Targeted Response Time shall be measured from the moment Care Quality Commission gives the written notice until the moment the CitizenLab support team acknowledges receipt of the notice. CitizenLab shall provide Support as outlined in this section set forth for specific priority levels in the table above.

1.3 In the event where CitizenLab fails to meet a Service Level Objective, Care Quality Commission shall be entitled, upon its written request, to the following Service Credits, which shall be compensated on the first month following such event:

- Service Availability <99%: reimbursement of 10% of the License Fee, prorated over a one-month period.
- Service Availability <99.5%: reimbursement of 5% of the License Fee, prorated over a one-month period.
- Service Availability <99.9%: reimbursement of 1% of the License Fee, prorated over a one-month period.
- Failure to meet a Targeted Response Time or a Targeted Resolution Time in the context of a Critical Service Issue: reimbursement of 10% of the Fee, prorated over a one-month period.
- Failure to meet a Targeted Response Time or a Targeted Resolution Time in the context of a Major Service Issue: reimbursement of 5% of the Fee, prorated over a one-month period.
- Failure to meet a Targeted Response Time or a Targeted Resolution Time in the context of a Minor Service Issue: reimbursement of 1% of the Fee, prorated over a one-month period.

1.4 If and insofar one or more Service Levels were not reached due to Force Majeure, the previous paragraph shall not apply.

1.5 The cumulative amount of Service Credits for a one-month period, shall not exceed the total Fee prorated over a one-week period, nor the amount for which CitizenLab's liability has been insured.

1.6 The Service Credits shall be applied to the portion of the Fee that was paid in the month wherein the Service Level Objective was not met.

2. Support hours and contact information

2.1 CitizenLab shall provide Priority Support to Care Quality Commission via telephone (using one of the phone numbers listed on CitizenLab's website), via email (support@citizenlab.co), or by responding to helpdesk tickets via the CitizenLab platform on Working Days.

Annex II.3: Privacy Policy

Controller of the processing of your personal data (hereafter: "the Organization"):

Name and legal form: Care Quality Commission

Belgian enterprise number:

Registered office address: [Deal Company.Address]

Contact e-mail address:

Processor on behalf of the Organization, and controller for the processing activities mentioned under 3.3 (hereafter: "CitizenLab"):

Name and legal form: CitizenLab NV

Belgian enterprise number: 0638.901.287

Registered office address: Anspachlaan 65, 1000 Brussels, Belgium

Contact e-mail address: support@citizenlab.co

Hereafter jointly referred to as "the Platform".

The Platform respects your privacy and strives to always treat your personal data with the necessary care and confidentiality. The Platform commits itself to comply with the General Data Protection Regulation ("GDPR") and any other applicable regulations.

Please find all relevant details below. Via the mentioned contact details, you can always reach the Platform for further questions or comments regarding the processing of your Personal Data.

1. SCOPE OF APPLICATION

This 'Privacy Policy' applies to the processing of your Personal Data through the Platform.

2. WHAT ARE PERSONAL DATA?

In this Privacy Policy, Personal Data refers to information that makes it possible to identify you. An identifiable person is someone who can be identified, either directly or indirectly, in particular by referring to an identification number or to one or more factors that are linked to physical, physiological, mental, economic, cultural or social identity. A typical example of Personal Data is your name and email address.

3. WHAT PERSONAL DATA DO WE COLLECT?

The Platform collects your Personal Data from the following three sources:

3.1. Personal Data that you provide during the registration process on the Platform, some of which are optional.

The Personal Data that the Platform collects from you are:

- First and last name
- E-mail address
- Year of birth
- Gender
- Area of residence
- Preferred language

This list can be extended on request of the Organization. If you choose to sign in via a third party authentication provider such as Google Accounts, Facebook or FranceConnect, they will provide us with the aforementioned Personal Data. The same applies if you choose to verify your identity with a third party identity provider as COW, FranceConnect or CSAM.

3.2. Personal Data that you provide when taking participative action on the Platform. Every action you take on the Platform (voting, posting an idea, writing a comment, answering a poll,...) constitutes Personal Data and is registered and stored. Such Personal Data is also linked to your registration data (3.1), implying that the Organization can link your platform profile to this participation data.

3.3. Personal Data that CitizenLab collects when you visit the Platform. CitizenLab (and third party processors acting on our behalf) collect information about the usage of the Platform for assessing the proper functioning and security of the platform. To this end, CitizenLab collects technical information that can identify you, such as your IP address and browser details.

We also gather usage data to improve our services.

The processing activities mentioned above are based on the legitimate interests of CitizenLab.

4. HOW DO WE USE PERSONAL DATA?

The Platform uses your Personal Data for the following purposes:

- First and foremost, to communicate your input to the Organization with relevant context, and to draw aggregated reports of all the data collected on this Platform to assist their decision-making.
- To create and maintain your user profile on the Platform.
- To manage the identification and authentication of users.
- To provide information about your community and/or alert you when activities on the Platform may interest you. You can opt-out of user emails from your user profile at any time.
- To improve the Platform and to monitor its functionalities.

The Personal Data is only stored and processed for the period required for the purpose of the processing. After that, the Personal Data will be deleted or anonymized.

5. WITH WHOM AND WHERE DO WE SHARE YOUR PERSONAL DATA?

CitizenLab shares your Personal Data with the Organization on behalf of which CitizenLab processes such Personal Data.

Where necessary the Platform engages external service providers who process Personal Data on its behalf, i.e. (sub-)processors. The Platform will only share your Personal Data with these external service providers to the extent necessary for the relevant purpose. The Personal Data may not be used for any other purposes by these third parties. In addition, these service providers are contractually bound to ensure the confidentiality of your Personal Data by means of a so-called "data processing agreement" concluded with these parties.

The Platform will never sell or rent your Personal Data to other service providers, nor will it share your Personal Data with any service provider that is not compliant with the GDPR.

Should the Platform, for limited and specific processing activities, rely on service providers that operate from outside the EEA, data transfers will only occur to countries from which the European Commission

has confirmed that they guarantee an adequate level of protection for your Personal Data, or where other measures have been taken to ensure the lawful processing of your Personal Data in these third countries.

6. WHAT ARE YOUR RIGHTS AS A DATA SUBJECT?

6.1. Right of access

You have the right to view your Personal Data at any time as well as the right to be informed of the use that the Platform makes of your Personal Data. You may also request a copy of the Personal Data that is being processed.

6.2. Right to rectification,

You have the right to obtain the rectification of inaccurate Personal Data that concerns you.

6.3. Right to erasure

You have the right to ask the Platform to delete your Personal Data. It is however possible that it is still necessary to process your Personal Data. When the Platform deletes your Personal Data, it may nonetheless retain a limited amount of Personal Data to ensure it can fulfill its obligations under the GDPR.

You acknowledge that a request for the erasure of Personal Data means that certain services may no longer be delivered.

If you choose to remove your account from the Platform, the Personal Data that was collected about you will be removed from our servers. Some Personal Data about you may remain in the logging data the Platform keeps for security and legal reasons for up to 30 days.

6.4. Right to object

You have the right to object to the processing of your Personal Data for serious and legitimate reasons. In addition, you always have the right to object to the use of your Personal Data for direct marketing purposes; in such cases, you do not have to state reasons.

6.5. Right to restriction of the processing

You can exercise your right to restrict the processing, if you believe that we process your Personal Data unlawfully. You can also request us to restrict the processing if you believe we process inaccurate Personal Data about you, for the period needed to verify the accuracy of your Personal Data. The same

applies when you exercise your right to objection to the processing of your Personal Data. In this case you can restrict the processing for the time needed to verify our legitimate grounds to process your data.

6.6. Right to data portability

You have the right to obtain the Personal Data you have provided to the Platform in a structured, typical and machine-readable form and/or have such transferred to different controllers.

6.7. Right to withdraw consent

Insofar the processing is based on your prior consent, you have the right to withdraw your approval.

6.8. Automated decision-making and profiling

The processing of your Personal Data does not include profiling and shall also not be subjected by Citizenlab to automated decision-making.

6.9. Right to lodge a complaint

You also have the right to lodge a complaint with a competent supervisory authority in the field of data protection. Hereunder we refer to the contact details of the Belgian Data Protection Authority. However, you can also lodge a complaint with the national supervisory authority of the EEA state where you have your habitual residence or place of work, or where the potential infringement occurred. For further information and the contact details of the supervisory authority of each EEA state, we refer to this web page of the European Data Protection Board.

Belgian Data Protection Authority
Drukpersstraat 35
1000 Brussels
Belgium
+32 (0)2 274 48 00
contact@apd-gba.be
Website DPA - file a complaint

Finally, you also have the option to file a legal claim against the Organization or against CitizenLab with the competent court in the EEA state where you have your habitual residence.

7. HOW TO EXERCISE YOUR RIGHTS?

You can exercise your rights by contacting:

- Either the Organization, by e-mail at ..., or by post to ..., provided you enclose a copy of the front of your identity card; or
- CitizenLab, by e-mail to support@citizenlab.co, or by post to Anspachlaan 65, 1000 Brussels, Belgium or by using the "Contact us" form on the Platform, provided you enclose a copy of the front of your identity card.

When you submit a request to exercise your rights, we will verify your identity if we have reasonable doubts in this regard. We do so to prevent your Personal Data from falling into the wrong hands. If we have doubts about your identity, we will request you to provide us with documents that enable you to identify yourself without a reasonable doubt, such as a copy of your identity card. In this case we urge you to cross out the non-relevant information for the verification of your identity, such as your national citizen number and photo.

Exercising your rights is in principle free of charge. However, if your request appears to be manifestly unfounded or excessive (in particular because of its repetitive character), we may charge you a reasonable fee to charge our own administrative costs. In such cases, we may also simply opt to reject your request. In this event, you will be notified of the reasons for such decision.

8. ADDITIONAL INFORMATION ON DATA COLLECTION AND PROCESSING

8.1. Legal procedures

CitizenLab and the Organization for whom we process your Personal Data may use the Personal Data for legal purposes, for the court or legal proceedings preceding phases in the event of unlawful use of this Application or the related services. You are aware that CitizenLab and the Organization it works with may be obliged to disclose the Personal Data at the request of competent government institutions for the processing of the Personal Data. The legal basis for this processing is the acceptance of the terms and conditions (contractual basis) and the necessity to fulfil a legal obligation.

8.2. Security Measures

The Platform has developed appropriate technological and organizational measures to prevent the destruction, loss, falsification, modification, prohibited access or the erroneous disclosure to third parties of Personal Data as well as any other prohibited processing of this Personal Data . Under no circumstances can the Platform be held liable for any direct or indirect loss resulting from the incorrect or unlawful use of your Personal Data by a third party. You must at all times comply with the security instructions, including by preventing all prohibited access to your login details and password. You are

solely responsible for the use made of the Platform on your computer, IP-address and your identification details, as well as for the confidentiality of such.

8.3. Changes to this privacy policy

The Platform reserves the right to change this privacy policy at any time by notifying the users on this page. We encourage you to check this page for possible changes. The date of the last change is indicated at the bottom of the page. If you object to any change in the policy, you must cease to use the Platform. Unless otherwise indicated, the valid Privacy Policy applicable at that time applies to all Personal Data that the Platform processes.

Annex II.4: Data Processing Agreement

Between: Care Quality Commission

*(*or other group company*)*

Here represented by its managing director *.

Hereafter: "*Controller*"

And: Citizenlab, Public Limited company under Belgian Law having its registered office at 1000 Brussels, Boulevard Anspach 65 (Belgium)and with enterprise number VAT BE0638.901.287;

Hereafter: "*Processor*"

Hereinafter jointly referred to as the 'Parties' or each separately as the 'Party'

TAKING INTO ACCOUNT THAT:

a) The Controller is the person who determines the purpose and means of processing personal data as specified in Appendix 1 of the Agreement;

b) The Controller wishes to instruct the Processor to perform the processing services as specified in Appendix 1 of the Agreement, and the Processor wishes to perform such processing services under the conditions set out in the Agreement.

c) This Agreement falls within the scope of the obligations arising from Article 28 of the General Data Protection Regulation of 27 April 2016 (hereinafter referred to as GDPR).

THE CONTRACTING PARTIES AGREE ON THE FOLLOWING:

Article 1 Definitions

Agreement: This processing agreement, regarding the processing of personal data and its annexes;

Service Agreement: the contract(s), other than this Agreement, entered into between the Parties, in which one or more data processing activities are processed by the Processor on behalf of the Controller;

Controller: As defined in the GDPR all natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, it may specify the Controller or the criteria for its designation;

Data breach/Infringement relating to Personal Data: a breach of security that accidentally or unlawfully results in the destruction, loss, alteration, unauthorised disclosure of or unauthorised access to transmitted, stored or otherwise processed Personal Data;

GDPR: General Data Protection Regulation (EU) 2016/679 of 27 April 2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC;

Personal Data: any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more elements specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person;

Processing: any operation or set of operations which is performed in relation to personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

Processor: As defined in the GDPR, all natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller;

Sub-Processor: this is the subcontractor appointed by the Processor to take on part of the processing process for the Controller;

Supervisory Authority: an independent government body responsible for monitoring compliance with the law in connection with the processing of Personal Data. In Belgium, this is the Data Protection Authority (GBA).

Article 2 Subject

This Agreement results from the obligation set out in Article 28 of the GDPR, which stipulates that a written contract must be drawn up between the Processor and the Controller.

This Agreement regulates the rights and obligations of the Controller and the Processor when processing Personal Data.

As of the entry into force of this Agreement, the Processor undertakes to comply with this Agreement when carrying out processing activities on behalf of the Controller. If processing activities already took place prior to the entry into force of the Agreement, the Processor undertakes, in any case as from the entry into force of the Agreement, to carry out these processing activities in accordance with the Agreement and to bring the processing activities carried out in reluctance to this Agreement into conformity with this Agreement within the shortest possible period of time.

Article 3 Contact details Data Protection Officer (DPO)

Mr. Franklin, Represented by Mr. Olivier Sustronck, lawyer, with office at Lieven Bauwensstraat 20, 8200 Bruges (Belgium), olivier@misterfranklin.be.

Article 4 Rights and obligations of the Processor

The Processor acts on the instructions of the Controller when processing Personal Data.

The Processor shall, in accordance with the instructions of the Controller, only process Personal Data as set out in Appendix 1 of the Agreement and in accordance with the provisions of the Service Agreement. The Processor shall only process such Personal Data that are strictly necessary for the execution of the Service Agreement and only such personal data listed in Appendix 1 of the Agreement.

The Processor shall train its staff responsible for Processing Personal Data with regard to applicable privacy laws in general and the GDPR in particular. The Processor shall use commercially reasonable efforts to ensure that its employees keep all Personal Data confidential and protected from unauthorised use.

The Controller agrees that the Processor has the ability to process the data of the platform as a Controller under the following conditions:

- The Processor will only process personal data when they have obtained a lawful processing

ground;

- The Processor will only use the data for internal use, for statistical purposes to improve the platform, for historical and scientific research, or for archiving purposes in the public interest, in accordance with Article 89 GDPR[1];
- Personal Data will not be Processed in a manner inconsistent with this Agreement;
- Appropriate technical and organizational measures will be taken to ensure respect for data minimization and include pseudonymisation and anonymization where possible.

Article 5 Rights and obligations of the Controller

The Controller undertakes to propose an addendum to this Agreement each time it issues a new processing order to the Processors or each time the purpose of the processing changes.

Article 6 Processing of personal data

6.1 The Processor and any Sub-processors, shall use commercially reasonable efforts to maintain the confidentiality of, and protect against the unauthorised use of the Personal Data it Processes.

6.2 The Personal Data may only be processed by the Processor for the purposes described in article 4 and Appendix 1 of the Agreement.

6.3 The Controller authorises the Processor to transfer Personal Data to Sub-processors pursuant to contracts that impose obligations that are equivalent to the obligations to which the Processor is subject under this Agreement.

6.4 The transfer of Personal Data by Processor to third parties other than those described in the previous paragraph is prohibited unless provided for by the applicable law or is instructed by court order. Processor shall notify Controller of all such transfers pursuant to this paragraph unless Processor is prohibited from doing so under such applicable law or court order.

6.5 The Processor may proceed to take a backup or a copy of the data on the platform.

Article 7 Rights of the party concerned

In the event that the Controller receives a request from the party concerned from whom Personal Data is being processed to exercise his rights in accordance with the GDPR such as e.g., the right to object or the

right to erase Personal Data, the Controller shall immediately pass on this instruction to the Processor.

The Processor undertakes to immediately and at the latest within fourteen (14) working days after receipt of the request, give an appropriate response to this instruction from the Controller and to either provide the requested information or make the requested adjustments to the Personal Data, or to remove and destroy certain Personal Data.

The Controller acknowledges and accepts that in the event that the data subject requests the deletion of the Data, the Processor will not necessarily be obliged to remove the Data from all its backups.

Article 8 Confidentiality

All Personal Data and information received by the Parties to this Agreement shall be treated as confidential for the duration of this Agreement and for ten (10) years thereafter, shall not be disclosed to third parties and shall not be used for any purpose other than to promote the objectives of this Agreement or the Service Agreement.

The obligation set out in the previous paragraph shall not apply to confidential information which:

- at the time of the disclosure by the disclosing Party was already publicly available or subsequently becomes publicly available without the action of the recipient;
- at the time of disclosure, was already in the legitimate possession of the recipient as sufficiently demonstrated by the recipient; or
- after disclosure by the recipient on a non-confidential basis, is received from third parties.
- Personal Data is also considered to be confidential information that cannot be used by the Processor at any time in the future, except under the conditions laid out in Article 4 of this Agreement.

Article 9 Liability and Guarantees

9.1 The Processor undertakes to strictly comply with the provisions of the Agreement when processing Personal Data and guarantees the Controller that it will take the necessary measures to ensure that its appointees charged with the execution of the Service Agreement comply with the provisions of this Agreement.

In particular, the Processor warrants the Controller that it has made its appointees aware of the provisions of the Agreement and has entered into an agreement with them that provides at least the warranties expected of the Processor in terms of the Agreement.

9.2 If the Processor is addressed by the Controller for damages as a result of non-compliance with this Agreement or Applicable Laws, the total liability of the Processor shall be limited to the total of the invoiced license and services in the previous calendar year. A series of related facts shall be considered as one event for the purposes of this Article.

9.3 The Processor shall not be liable for any form of indirect damage such as, but not limited to, business interruption, reduced goodwill, lost savings, lost profit, reputational damage or any other form of indirect, incidental or consequential damage, regardless of the nature of the act.

Article 10 Duration, Cancellation and Termination

This Agreement forms an integral part of the preceding Service Agreements concluded between the Parties and is to be regarded as a supplement to or amendment to them and takes precedence over all other agreements between the Parties. Parties shall amend this Agreement to reflect changes or additions to regulations, additional instructions from the relevant authorities, and progressive understanding of the application of Privacy laws (for example, by, but not limited to, case law or advice from the Data Protection Authority or the European Data Protection Supervisor (EDPS)).

This Agreement is entered into for the duration of the Service Agreement(s).

Article 11 Effects of termination

Immediately upon termination of the Service Agreement or expiration of the retention period, the Processor shall - on the explicit request of the Controller - transfer the Personal Data to the Controller and/or completely and irrevocably erase the Personal Data, and delete the existing copies.

In the event of the Controller's silence regarding the fate of the Personal Data after the termination or expiration of the Services Agreement, the Processor shall delete the Personal Data at the end of a three (3)-month period starting from the termination or expiration of the Services Agreement. Anonymization, in which case the Processor eliminates Personal Data by ensuring that data subjects can no longer be identified, is an acceptable process hereto.

The Processor may deviate from the first paragraph if the storage of the Personal Data is required by European or national legislation.

Article 12 Monitoring by Controller

The Controller is entitled to monitor compliance with the Processing Agreement. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the provisions of this Agreement and shall allow the Controller or an auditor authorised by the Controller to carry out audits and inspections, or to assist the Controller in doing so. A notification of the audit must be given at least one (1) month in advance.

The costs of this audit will be borne in full by the Controller.

Article 13 Security

The Processor undertakes to take the appropriate technical and organizational measures to secure Personal Data and the processing thereof in accordance with Appendix 2 of the Agreement.

The Processor undertakes to take the necessary steps to limit access to Personal Data only to staff members employed by the Processor who require access to such Personal Data in order to execute the Service Agreement.

Article 14 Sub-Processors

In case the Processor wishes to appeal to a Sub-Processor within the meaning of this article, the Processor undertakes to enter into a written agreement with this Sub-Processor that includes at least the guarantees and obligations arising from this agreement. The Processor shall keep an up-to-date register of third parties and Sub-Processors employed by them, which includes the identity, place of business and a description of the activities of the third parties or Sub-Processors, as well as any additional conditions imposed by the data Controller.

This register shall be added as Appendix 4 to this Processing Agreement and shall be kept up to date by the Processor.

Article 15 Miscellaneous provisions

15.1 This Agreement covers the entire agreement between the Parties concerning the subject matter thereof and replaces all previous written and oral agreements.

15.2 In the event of any inconsistency between this Agreement and the Service Agreement(s) to which it relates, this Agreement shall take precedence over the latter.

15.3 This Agreement may be supplemented, amended, or modified only by the mutual consent of the Parties. No supplement, modification, or amendment to this Agreement shall be binding unless it is in writing and signed by both Parties.

15.4 If one or more provisions of this Agreement should be declared null and void or become unenforceable, the legality, validity and enforceability of the remaining provisions of this Agreement and of the Agreement as a whole, to the extent that they still have any effect or reason for existence, shall not be affected.

The parties undertake, to the extent legally possible, to replace the invalid provisions with new provisions that are consistent with the objectives and choices of this Agreement.

15.5 Neither Party may transfer the rights under this Agreement to third parties without the prior written consent of the other Party. Adjustments or amendments to this Agreement shall only take place if they are accepted and signed in writing between both Parties.

Article 16 Data breach

Should a Data Breach be detected, the Processor shall inform the Controller as soon as possible and at the latest within 48 hours after the discovery by contacting the contact person designated by the Service Agreement as well as the DPO (see Article 3). The Processor shall under no circumstances inform the parties involved about this Data Breach, without prejudice to the obligation to undo or limit the consequences of such infringements and incidents as soon as possible.

In addition, at the Controller's first request, the Processor shall provide all information that the Controller considers necessary to assess the incident.

The Processor undertakes to inform the Controller, after detecting a Data Breach, of any measures taken to limit the extent of the Data Breach or to avoid similar breaches in the future.The Processor has a thorough plan of action concerning the handling and settlement of data breaches and will, at the request of the Controller, grant the Controller access to the plan. The Processor shall notify the Controller of any

material changes to the plan of action.

The Processor will provide all necessary assistance in providing additional information requested by the Supervisor(s) and/or the Data Subject(s) as soon as possible, if necessary. In doing so, the Processor shall at least provide the information as described in Appendix 3 to the Controller.

The Processor shall keep a detailed register of all (suspected) data breaches, as well as the measures taken following such breaches, in which at least the information referred to in Appendix 3 is included, and shall grant access to this at the Controller first's request.

Article 17 Data outside the EU

The Processor undertakes to always obtain the necessary guarantees from the Sub-processors, if Personal Data that depend on this Agreement are processed outside the EU. The Processor declares that processing shall always be carried out in accordance with the provisions set out in Articles 44 et seq. of the GDPR.

Article 18 Assistance

The Processor shall assist the Controller in fulfilling its obligations under the GDPR. The Processor shall assist the Controller in carrying out a Data Protection Impact Assessment in accordance with Articles 35 and 36 of the GDPR.

Article 19 Applicable law and disputes

This Agreement shall in all respects be governed by, and construed and interpreted in all respects by the laws of Belgium.

Disputes concerning the execution or interpretation of the Agreement shall be submitted exclusively to the courts having jurisdiction over the registered office of the Controller.

Brussels, Aug 05, 2021
Made in 2 copies
(signatures follow)

CitizenLab	**Care Quality Commission**
Dated	Dated
Processor	Controller

[1] Article 89 GDPR. "Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes."

Appendix 1: Overview of Personal Data, Nature of Processing and Processing Purposes

A. In what context are the personal data processed by the Processor:

Personal data is processed to enable users to register and participate via various participation methods on the platform.

B. What type of personal data are processed:

Type of personal data	**Nature of processing operation**	**Objective of processing operation**	**Categories**
Name	To administer the list of participants	User administration	All users
Email	To keep users informed on their contribution	User administration	All users
IP Address	To administer a list for third party processing	User administration	All users
Gender *(optional)*	To gain insights on demographic representativeness and voting preferences	Collection of statistical information	All users
Year of birth *(optional)*	To gain insights on demographic representativeness and voting preferences	Collection of statistical information	All users

Area of residence *(optional)*	To gain insights on demographical representativeness and voting preferences	Collection of statistical information	All users
Participant contributions (ideas, comments, votes and surveys)	To allow users to participate	Online participation	All users
Avatar image (optional)	To let users specify their own visually recognizable identity towards others	Online participation	All users

Appendix 2: Overview of Security Measures

Taking into account the state of the art, the cost of implementation, and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (Art. 32 GDPR).

The Controller shall require the Processor to take measures which include, inter alia, the following:

- Pseudonymisation and encryption of personal data.
- Ability to ensure the integrity, availability and confidentiality of processing systems on a permanent basis.
- The ability to restore the availability of and access to personal data in the event of a physical or technical incident.
- A procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to secure processing.

Description of the technical and organizational measures:

Technical measures

Anonymisation and pseudonymisation

- The presence of automatic anonymisation or pseudonymisation of personal data (after the processing purpose or the retention period has been exceeded).

User management

- The user can choose his/her own password taking into account the password requirements such as length, special characters, etc.
- The user can reset his/her own password via profile settings
- The ability to provide access restriction to processing and/or data for unauthorised users

Audit and evaluation possibilities

- The Processor maintains logs of user activity, accessed by authorized personnel only.
- Procedures for periodic evaluation of existing IT processes

Backup

- The Processor performs a daily (nightly) backup of the platform data and application. Backups are encrypted and automatically removed after 30 days.
- The Processor can check the integrity of the backups via the server interface.

Data exchange

- Personal data is made available via a secure connection (https, VPN, IPSEC, FTPS, encrypted email, etc.).
- Physical data supports (USB sticks, external HDDs, etc.) are encrypted.

Organizational measures

- A safety consultant/DPO has been appointed
- Policy on *clear screen, clean desk*
- Policy on external devices (laptops, USB sticks, etc.)
- Data destruction policy
- Training received by staff in relation to the GDPR can be demonstrated.
- Data breach policy
- Company devices are provided with a password and equipped with an up-to-date virus scanner

Appendix 3 Summary of information relating to an incident

The Processor shall provide at least the following information to the Controller in the event of an incident involving personal data of the Controller:

- What the (alleged) cause of the infringement is;

- What the (as yet known and/or expected) consequences are;
- What the (proposed) solution is;
- Contact details for follow-up of the report;
- Number of persons whose data is involved in infringement (if no exact number is known: the minimum and maximum number of persons whose data is involved in the infringement);
- A description of the group of persons whose data is involved in the infringement;
- The type or types of personal data involved in the breach;
- The date on which the infringement took place;
- The period during which the infringement took place (if no exact date is known);
- The date and time on which the infringement became known to the processor or to a third party or subcontractor engaged by him;
- Whether the data has been encrypted, hashed or otherwise made incomprehensible or inaccessible to unauthorised persons;
- What measures have already been taken to bring the infringement to an end and to limit its effects.

Appendix 4: Overview of Subprocessors

Name	Type	Address	Optional?	Host location	Purpose	Personal data through	What personal data?
AWS	IaaS	**One Burlington Plaza, Burlington Road, Dublin 4**	No	EU (Frankfurt)	Data and application server hosting	Hosting	Everything
DigitalOcean	IaaS	**New York 101 6th Avenue**	No	EU (Frankfurt and Amsterdam)	Supporting web services hosting	Hosting	Everything
Intercom	SaaS	**3rd Floor, Stephens Ct., 18-21 St. Stephen's Green, Dublin 2**	Yes	US (AWS N. Virginia) (SCC)	Communicating with CitizenLab customers	Hosting + Email	Only admins and moderators
Salesmachine	SaaS	**9 Villa Wagram Saint Honor´, 75008 PARIS**	Yes	EU	Following up on CitizenLab customers to support them	Intercom	Only admins and moderators
Typeform	SaaS	**Carrer de Bac de Roda, 163, 08018 Barcelona, Spain**	Yes	US (AWS N. Virginia) (SCC)	Rich surveys embedded on the platform	Embedded as iframe	Email is passed as a parameter to the iframe

citizenlab

Quote

Name	Type	Address	Optional?	Host location	Purpose	Personal data through	What personal data?
Facebook Pixel	SaaS	4 Grand Canal Square, Dublin 2 Dublin	Yes	US (SCC)	Facilitate advertisement campaigns to boost citizen engagement	Google Tag Manager	User visits
Google Ads	SaaS	Chaussee d'Etterbeek 180 1040 Brussels Belgium	Yes	US (SCC)	Facilitate advertisement campaigns to boost citizen engagement	Google Tag Manager	User visits
Zapier	SaaS	548 Market St. #62411, San Francisco, CA 94104-5401	Yes	US (SCC)	Middleware to connect other tools	Intercom	Only admins and moderators
CloudAMQP	IaaS	Sveavägen 98, 113 50 Stockholm, Sweden	No	EU (AWS Dublin)	Middleware hosting to connect internal application components	Hosting	Everything
Mailgun	SaaS	112 E Pecan St #1135, San Antonio, TX 78205, United States	No	EU/US (SCC)	Send platform emails	Code integration	email address, name, occasional additional personal data

Name	Type	Address	Optional?	Host location	Purpose	Personal data through	What personal data?
Satismeter	SaaS	Česká 1113/1, Prague 5, 158 00, Czechia	Yes	US (AWS N. Virginia) (SCC)	Collect customer satisfaction score	Code integration	Only admins and moderators
Google Tag Manager	Saas	Chaussee d'Etterbeek 180 1040 Brussels Belgium	Yes	US (SCC)	Middleware to connect other tools	Code integration	User visits