TERMS AND CONDITIONS

1. Definitions and interpretation

1.1. In the Services Agreement:

"**Affiliate**" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with another entity.

"**Applicable Law**" means all applicable laws and regulations, as amended and in force from time to time.

"**Business Day**" means a day other than a Saturday, Sunday or public holiday in England, when banks in London are open for business.

"**Charges**" means the charges set out in the Order Form (the Licence Fee, the Project Fee and any other charges set out in the Order Form), and any applicable pause fee detailed in Schedule 3.

"**Closed**" means in respect of a Customer Commonplace, that it has been closed to members of the public for comment and "**Closing**" shall be interpreted accordingly.

"**Commonplace**" means **Commonplace Digital Ltd** (company number 08575062) of 30 Old Bailey, City of London, London EC4M 7AU, United Kingdom, or any of its affiliates.

"**Commonplace Business Processes'** means activities that the Commonplace team carries out to continually improve its product, service and operations, which may include such activities as staff training and product development.

"**Commonplace Contact**" means the person set out in the Order Form (or as updated by Commonplace from time to time).

"**Commonplace Platform**" means the platform which facilitates local community engagement, social listening and representative surveys, as made available by Commonplace as part of the Zencity group, from time to time, in accordance with its standard roadmap.

"**Commonplace Privacy Policy**" means the privacy policies of Commonplace and Zencity available at: https://www.commonplace.is/privacy-policy and https:/zencity.io/privacy-policy/.

"**Control**" in respect of a company, the power of a person to directly or indirectly secure: (a) by means of the holding of shares or the possession of voting power in or in relation to that company or any other body corporate; or (b) by virtue of any powers conferred by the articles of association or other document regulating that company or any other body corporate, that the affairs of the company are conducted in accordance with the wishes or directions of that other person.

"**Customer**" means the customer identified in the Order Form.

"**Customer Contact - General**" means the person identified in the Order Form (or as updated by Customer from time to time).

"**Customer Contact – Legal and Data Protection**" means the person identified in the Order Form (or as updated by Customer from time to time).

"**Customer Deadlines**" means the deadlines which Customer must meet as set out in the Order Form.

"**Customer Input**" means any materials which Customer and/or Partners have provided to Commonplace, including Customer Properties.

"**Customer Output**" means any materials which Customer or anyone authorised by Customer has downloaded from the Commonplace Platform using the functionality made available by Commonplace to enable Customer to do so (but excludes any other materials extracted by anyone without Commonplace's authorisation).

"**Customer Properties**" means the materials listed in the Order Form.

"**Documentation**" means the online user guides and help made available by Commonplace for its customers from time to time.

"**Go Live Date**" means the date upon which Commonplace notifies Customer [in writing] that Customer Commonplaces are live.

"**Harmful Element**" means any code which is designed to disrupt, disable, harm or otherwise impede in any manner, including aesthetic disruptions or distortions, the operation of any of any hardware, software, firmware, computer system or network on which it is installed or with which it interacts, or that would permit Customer or any other person to access systems to cause such disablement or impairment, or which contains any other similar harmful, malicious or hidden procedures, routines or mechanisms which would cause such programs to cease functioning or to damage or corrupt data, storage media, programs, equipment or communications, or otherwise interfere with operations including computer programs commonly referred to as worms or Trojan horses (whether or not specifically directed at Commonplace).

"**Intellectual Property Rights**" means all vested and future rights of copyright and related rights, design rights, database rights, patents, rights to inventions, trade marks and get-up (and goodwill attaching to those trade marks and that get up), domain names, applications for and the right to apply for any of the above, moral rights, goodwill (and the right to sue for passing off and unfair competition), rights in know-how, rights in confidential information, rights in computer software, and any other intellectual or industrial property rights or equivalent forms of protection, whether or not registered or capable of registration, and all renewals and extensions of such rights, whether now known or in future subsisting in any part of the world.

"**Licence Fee**" means the licence fee for the Products set out in the Order Form.

"**Local Areas**" means the local areas in relation to which Customer wishes to gather feedback and opinions as set out in the Order Form.

"**Losses**" means claims, demands, actions, awards, judgments, settlements, costs, expenses, liabilities, damages and losses (including all interest, fines, penalties, management time and legal and other professional costs and expenses).

"**Order Form**" means the order form between Commonplace and Customer to which these Terms and Conditions apply.

"**Partners**" means any third parties to whom Customer has given access to the Commonplace Platform, and shall include the Project Partners.

"**Product(s)**" means the products identified in the Order Form.

"**Project Fee**" means the fee for the Project Services set out as such in the Order Form.

"**Project Partners**" means the partners listed in the Order Form.

"**Project Services**" means the services described in the Order Form.

"**Service Levels**" means the service levels set out.

"**Services**" means the services set out in the Order Form, including the Products and Project Services.

"**Services Agreement**" means together the Order Form and the Terms and Conditions, as varied, novated, supplemented, amended, or replaced from time to time in accordance with its terms.

"**Start Date**" means the date the Term commences as set out on the Order Form.

"**Target Go Live Dates**" means the target dates for Customer Commonplaces to go live as set out on the Order Form.

"**Term**" means the period beginning on the Start Date as set out on the Order Form.

"**Terms and Conditions**" means the then current terms and conditions of Commonplace.

1.2. In the Services Agreement the interpretation of general words shall not be restricted by words indicating a particular class or particular examples.

2. TERM

The Services Agreement begins on the Start Date and shall continue for the Term, unless terminated earlier in accordance with its terms.

3. SERVICES AND SERVICE LEVELS

3.1. Subject to payment of the Charges in accordance with clause 7, Commonplace shall provide the Services in accordance with the Services Agreement. Commonplace shall not be obliged to provide any element of the Services prior to payment of the applicable Charges.

3.2. Commonplace shall configure the Products for the Local Areas to make Customer Commonplaces available using the Commonplace Platform.

3.3. Commonplace shall provide the Project Services.

3.4. Commonplace shall use reasonable endeavours to meet the Target Go Live Date.

3.5. In performing its obligations under the Services Agreement, Commonplace shall apply such time, attention and skill as may be reasonable, taking into account the resources available to Commonplace, for the due and proper performance of the Services with the reasonable care and skill to be expected of a similar software as a service provider.

3.6. Commonplace shall, on a day to day basis, manage all activities under the Services Agreement via Customer Contact.

3.7. Commonplace shall use reasonable endeavours to remedy any failure to meet the Service Levels as soon as reasonably possible by taking all reasonable steps to ensure that such service failure does not recur.

4. CUSTOMER COMMONPLACES

4.1. Each Customer Commonplace will be open to accept comments from members of the public for 12 months from Go Live Date or such shorter period as instructed by Customer.

4.2. Comments from members of the public will be subject to the Commonplace Privacy Policy.

4.3. Once comments have been Closed, Commonplace shall continue to host Customer Commonplace for 12 months ("**Closed Period**").

4.4. During the Closed Period Customer may continue to access data using the Commonplace Platform, but not thereafter.

5. CUSTOMER RESPONSIBILITIES

5.1. Customer shall give Commonplace all reasonable and necessary assistance to enable Commonplace to provide the Services, including by: (a) providing Commonplace with Customer Properties; (b) using reasonable endeavours to meet Customer Deadlines and c) promoting the availability of the Customer Commonplaces to the public and stakeholders.

5.2. Customer shall ensure that all Customer Properties provided or made available in electronic form do not contain any Harmful Elements.

5.3. Customer shall, on a day to day basis, manage all activities under the Services Agreement via the Commonplace Contact.

5.4. Customer acknowledges and agrees that Commonplace cannot provide the Services in accordance with the Services Agreement without co-operation from both Customer and Partners. Commonplace shall keep Customer informed of any interference or delay to its ability to deliver the Services. Customer shall use its best endeavours to remove the interference of delay, including any caused by a Partner.

5.5. Customer shall, and shall procure that Partners shall, use the Services in accordance with the Service Agreement, including the Documentation.

5.6. Customer shall be responsible for all activities of Partners and all activities of persons given login credentials by or on behalf of Customer or a Project Partner.

5.7. If Customer believes that anyone has unauthorised access it shall notify Commonplace immediately so that the login can be revoked.

6. FEATURES, ROADMAP AND COLLABORATION

6.1. Commonplace provides services to its customers via the Commonplace Platform on a software as a service basis. Whilst retaining the overall nature of the Commonplace Platform, when taken as a whole, Commonplace reserves the right to change, update, upgrade or discontinue features of the Commonplace Platform in its absolute discretion at any time. Customer can view the current features of the Commonplace.

6.2. Commonplace may from time to time share its roadmap for its services, including plans to add/remove features, its functionality priorities and other information. Commonplace welcomes feedback from Customer and its partners on its roadmap.

6.3. Customer shall meet with Commonplace as reasonably requested by Commonplace to provide feedback on the Services for the purpose of planning the future roadmap.

6.4. If Customer provides any technical or other information to Commonplace, Commonplace has an unrestricted right to use such information for its business purposes, including for support and product/service development.

7. CHARGES AND PAYMENT

7.1. Customer shall pay Commonplace the Charges.

7.2. The Charges do not include value added tax or any locally applicable equivalent sales tax, which Customer shall pay, in addition to the Charges, without set-off or withholding (and if withholding is required by Applicable Law, Customer shall gross up its payment accordingly).

7.3. Commonplace shall invoice Customer the Charges as follows: (a) Licence Fee: upon signature of the Services Agreement and at least 14 days in advance of the relevant Renewal Term; and (b) Project Fee: as set out in the Order Form; and (c) any other charges as set out in the Order Form or otherwise agreed in writing between Commonplace and Customer.

7.4. Unless the subject of a genuine dispute, Customer shall pay all invoices within 14 days of the date of the invoice.

7.5. If a party fails to pay in full on the due date any sum payable by it under or in connection with the Services Agreement, interest on the outstanding amount shall accrue on a daily basis from the due date until the date of payment (whether before or after judgment) at the rate of 2% per annum above the base rate of Barclays Bank PLC from time to time.

7.6. If Customer does not pay on time Commonplace may suspend use of the Services (including Closing any live Customer Commonplaces) until payment is made.

7.7. Commonplace reserves the right to make annual inflationary increases to the Charges, in line with the Retail Price Index.

8. INTELLECTUAL PROPERTY RIGHTS

8.1. Customer may only access and use the Commonplace Platform and Services for its own internal business purposes. Partners may only access and use the Commonplace Platform in support of Customer's use.

8.2. Customer acknowledges and agrees that Commonplace and/or its licensors own all Intellectual Property Rights in the Commonplace Platform and the Services. Customer's use of any such Intellectual Property Rights is limited to that required to receive and make use the Services as envisaged by the Services Agreement.

8.3. Unless permitted and necessary under Applicable Law, Customer may not copy, modify, adapt, redistribute, decompile, reverse engineer, disassemble, or create derivative works of any software or content made available by Commonplace or any component of such software or content. Customer may not use any work around to seek to circumvent any technical limitations.

8.4. Customer hereby grants to Commonplace a worldwide, royalty-free right to ingest, adapt, copy, communicate to the public and otherwise use and exploit Customer Input for the purposes of delivering the Services and Commonplace Business Processes..

8.5. Subject to clause 11.1, Commonplace hereby grants to Customer a worldwide, royalty-free right to access, download, ingest, adapt, copy, communicate to the public and otherwise use and exploit Customer Output.

8.6. Each party ("**Infringing Party**") shall on demand indemnify the other party from and against all Losses incurred by that party ("**Indemnified Party**"), its employees, officers, agents and contractors arising out of or in connection with any claim, demand or action alleging that the Infringing Party has infringed any Intellectual Property Rights of a third party.

8.7. Indemnified Party shall notify Infringing Party promptly in writing of any third party action, demand or claim under clause 8.6 ("**Claim**") of which it is aware and shall: (a) at its option, give Infringing Party express authority to conduct all negotiations and litigation, and settle all litigation, arising from the Claim; and (b) in relation to any claim which Infringing Party conducts, provide Infringing Party with all such available information and assistance as Infringing Party may reasonably require, at Infringing Party's expense.

8.8. If, within 30 days after Infringing Party's receipt of notice of any Claim, Infringing Party fails to take reasonable action to defend the same, and such Claim is not withdrawn, Indemnified Party may at Infringing Party's reasonable expense undertake the defence, compromise or settlement of the Claim. Upon the assumption of the defence of the Claim, Indemnified Party may defend, compromise or settle the Claim as it sees fit, provided that Indemnified Party agrees to take reasonable steps to monitor and mitigate the fees and costs associated with the same and to keep Infringing Party informed of any reasonable settlement proposals made by the claimant.

8.9. Infringing Party shall not use Indemnified Party's name in any action or claim without Indemnified Party's prior written consent.

8.10. Infringing Party shall not make any admission as to liability or agree to any settlement or compromise of any Claim without the prior written consent of Indemnified Party (not to be unreasonably withheld or delayed).

9. THIRD PARTY DATA AND SERVICES

9.1. Customer acknowledges that all third-party data and services which it or partners or users may access through use of Customer Commonplaces are the sole responsibility of the person from which they originated.

9.2. Customer acknowledges that use of third party data and services may be subject to separate terms between Customer and the relevant third party. In that case, the Services Agreement does not affect Customer's legal relationship with these third parties.

10. WARRANTIES

10.1. Except as expressly set out in the Services Agreement, neither Commonplace nor any of its suppliers, partners or investors make any specific promises about the Services.

10.2. Except as expressly set out in the Services Agreement, Commonplace does not warrant that any of the Services will be secure, accurate, uninterrupted or error free or that they will meet Customer's or any third party's specific requirements.

10.3. Each party represents and warrants that it has the power and authority to enter into and perform its obligations under the Services Agreement, which constitutes valid and binding obligations on it in accordance with its terms.

10.4. Commonplace represents and warrants that: (a) the provision of the Services by Commonplace to Customer shall not infringe the Intellectual Property Rights of a third party in the United Kingdom; and (b) in performing its obligations under the Services Agreement it shall comply with all Applicable Law.

10.5. Customer represents and warrants that: (a) it has in place all necessary licences and permissions to deliver Customer Input and to receive the Services; (b) in performing its obligations under the Services Agreement it shall comply with all Applicable Law (including relating to Intellectual Property Rights); and

(c) it is not entering into the Services Agreement so as to gain access to confidential information or intellectual property with the intention of developing a service the same as or similar to the Commonplace Platform.

11. Data Protection

11.1. Each party shall comply with the Data Processing Addendum set out in Schedule 1.

12. CONFIDENTIALITY and announcements

12.1. "**Confidential Information**" means all information of a confidential nature in the disclosing party's possession or control, whether created before or after the date of the Services Agreement, whatever its format, and whether or not marked "confidential"; and terms of the Services Agreement, but not including information which is or comes into the public domain through no fault of the other party, was already lawfully in the other party's possession or comes into the other party's possession without breach of any third party's confidentiality obligation to the disclosing party, or is independently developed by or on behalf of the other party.

12.2. Each party shall safeguard the other party's Confidential Information as it would its own confidential information, and shall use, copy and disclose that Confidential Information only in connection with the proper performance of the Services Agreement.

12.3. Nothing in the Services Agreement shall be construed so as to prevent one party from disclosing the other's Confidential Information where required to do so by a court or other competent authority, provided that, unless prevented by Applicable Law, the first party promptly notifies the other party in advance and discloses only that part of the other party's Confidential Information that it is compelled to disclose.

12.4. Commonplace may publicly use Customer's name and logo, and references to Customer Commonplaces, to refer to Customer as a customer of Commonplace. Commonplace will follow any applicable brand usage guidelines provided by Customer.

13. Limitations on liability

13.1. Subject to clauses 13.2, 13.3 and 13.4, the total liability of each party to the other in connection with the Services Agreement, whether arising from contract, negligence or otherwise, shall be limited to 125% of the applicable Charges paid by Customer to Commonplace.

13.2. Subject to clause 13.4, neither party shall be liable for any indirect or consequential loss.

13.3. The limitation of liability for the indemnity in clause 8.6 shall be limited to the amount recoverable under the Indemnifying Party's insurance.

13.4. The exclusions and limitation of liability set out in clause 13 do not apply to: (a) liability arising from death or injury to persons caused by negligence; (b) Customer's obligation to pay the Charges; (c) liability arising as a result of fraud;

14. insurance

Commonplace shall maintain in force at its own expense all insurances required by Applicable Law with a reputable insurer.

15. Termination

15.1. Either party may terminate the Services Agreement with immediate effect by giving written notice to the other party if: (a) the other party commits a material breach of the Services Agreement which is not capable of remedy (or is capable of remedy, but which the other party fails to remedy within 30 days of receiving notice specifying the breach and requiring the breach to be remedied); or (b) the other party repeatedly breaches any of the terms of the Services Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms of the Services Agreement.

15.2. Commonplace may terminate the Services Agreement if Customer commits a breach of clause 7 and Customer does not remedy the relevant breach within 10 Business Days of receipt of written notice of the breach being given by Commonplace.

15.3. Either party may terminate the Services Agreement with immediate effect by giving the other party notice if: (a) such other party becomes unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986 (as amended); (b) such other party ceases or threatens to cease to carry on the whole or a substantial part of its business; (c) any distress or execution shall be levied upon such other party's property or assets; (d) such other party shall make or offer to make any voluntary arrangement or composition with its creditors; (e) any resolution to wind up such other party (other than for the purpose of a *bona fide* reconstruction or amalgamation without insolvency) shall be passed, any petition to wind up such other party shall be presented and not withdrawn or dismissed within seven days or an order is made for the winding up of such other party; (f) such other party is the subject of a notice of intention to appoint an administrator, is the subject of a notice of appointment of an administrator, is the subject of an administration application, becomes subject to an administration order, or has an administrator appointed over it; (g) a receiver or administrative receiver is appointed over all or any of such other party's undertaking property or assets; (h) any bankruptcy petition is presented or a bankruptcy order is made against such other party; (i) an application is made for a debt relief order, or a debt relief order is made in relation to such other party; (j) such other party is dissolved or otherwise ceases to exist; or (k) the equivalent of any of the events described in (a) to (j) occurs in relation to such other party under the laws of any jurisdiction.

15.4. For the purposes of clause 15, a breach shall be considered capable of remedy if the party in breach can comply with the provision in question in all respects other than as to the time of performance.

15.5. Termination or expiry of the Services Agreement (howsoever occurring) shall not affect either of the parties' accrued rights or liabilities, or the coming into force or the continuance in force of any provision which is expressly or by implication intended to come into or continue in force on or after termination or expiry.

16. Termination assistance

Immediately after receipt (or service) of notice to terminate the Services Agreement under clause 15, each party shall provide all reasonable assistance and information to the other to ensure an orderly end to the relationship.

17. Force majeure

Neither party shall be liable for any breach of the Services Agreement directly or indirectly caused by circumstances beyond the reasonable control of that party and which prevent that party from performing its obligations to the other, provided that a lack of funds shall not be regarded as a circumstance beyond that party's reasonable control.

18. ANTI-CORRUPTION

18.1. Each party warrants that it is not aware of any financial or other advantage being given to any other person working for or engaged by that party in connection with the Services Agreement which is or may be in breach of the Bribery Act 2010 ("**BA**").

18.2. Each party shall, if requested by the other party, provided reasonable assistance to the other party (at requesting party's expense), to enable that party to perform any activity required by any government or agency to comply with the BA.

19. FREEDOM ON INFORMATION

19.1. If Customer is a public authority for the purposes of the Freedom of Information Act 2000 ("**FOIA**"), Commonplace shall reasonably assist and co-operate (at Customer's expense) to enable Customer to comply with any relevant and lawful request for information under FOIA.

19.2. Customer shall comply with all of Commonplace's reasonable requests to exempt and/or redact information subject to Applicable Law.

19.3. Commonplace acknowledges that the Customer may, acting in accordance with the Secretary of State for Constitutional Affairs' Code of Practice on the discharge of public authorities' functions under Part 1 of FOIA (issued under section 45 of the FOIA, November 2004), be obliged under the FOIA or the Environmental Information Regulations to disclose Information:

(a) without consulting with Commonplace, or

(b) following consultation with Commonplace and having taken its views into account

20. GENERAL

20.1. This Agreement is not assignable or transferable by either party without the other party's prior written consent, provided however that either party may assign this Agreement to a successor to all or substantially all of its business or assets.

20.2. Customer shall not, without the written consent of Commonplace (which shall not be unreasonably withheld or delayed) assign or transfer any of its rights or obligations under the Services Agreement to any third party who is not an Affiliate of Customer.

20.3. Nothing in the Services Agreement is intended to or shall operate to create a partnership or joint venture of any kind between the parties. No party shall have the authority to bind the other party or to contract in the name of, or create a liability against, the other party in any way or for any purpose.

20.4. The parties do not intend any third party to have the right to enforce any provision of the Services Agreement under the Contracts (Rights of Third Parties) Act 1999 or otherwise.

20.5. The Services Agreement is the entire agreement between the parties, and replaces all previous agreements and understandings between them, relating to its subject matter.

20.6. No variation of the Services Agreement shall be effective unless it is in writing and signed by or on behalf of each party.

20.7. The rights and remedies expressly conferred by the Services Agreement are cumulative and additional to any other rights or remedies a party may have.

20.8. Notices under clause 15 shall be in writing and delivered by hand or sent by recorded delivery post to the relevant party at its address as set out in the Services Agreement. Without evidence of earlier receipt, notices are deemed received: (a) if delivered by hand, at the time of delivery; (b) if sent by recorded delivery, at 9.00 am on the second Business Day after posting; and (c) in the case of post it shall be sufficient to prove that the notice was properly addressed and posted or transmitted. Any other notices and communications under the Services Agreement may be delivered in writing and/or electronically.

20.9. The Services Agreement and any non-contractual obligations arising in connection with it are governed by and construed in accordance with English law, and the English courts have exclusive jurisdiction to determine any dispute arising in connection with the Services Agreement, including disputes relating to any non-contractual obligations.

Schedule 1: Data Processing Addendum

The purpose of this Data Processing Addendum ("**DPA"**) is to set out each party's obligations relating to the personal data processed by the parties pursuant to the **Services Agreement** entered into between them and into which this DPA is incorporated.

1. **Definitions**

Defined terms in the Services Agreement have the same meaning where used in this DPA unless otherwise defined below.

Appropriate Safeguards	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time currently (i) A transfer to a third country of an international organization may take place where it is based on adequacy regulations (see section 17A of UK GDPR); (ii) there are appropriate safeguards in place pursuant to Article 46 UK GDPR; (iii) Binding corporate rules are in place; or (iv) one of the derogations for specific situations in Article 49 UK GDPR applies to the transfer;
Applicable Law	means as applicable and binding on Customer, Commonplace and/or the Services: (i) any law, statute, regulation, by-law or subordinate legislation in force from time to time to which a party is subject; (ii) any court order, judgment or decree; or (iii) any direction, policy, rule or order that is made or given by any regulatory body having jurisdiction over a party;
Controller	means the entity which determines the purposes and means of the Processing of Personal Data; For the purpose of clarity, within this DPA "**Controller**" shall also mean "**Business**", and "**Processor**" shall also mean "**Service Provider**", to the extent that the CCPA applies. In the same manner, Processor's Sub-processor shall also refer to the concept of Service Provider**.**
Data Protection Laws	means all privacy and data protection laws and regulations, including such laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, Canada, Israel and the United States of America, as applicable to the Processing of Personal Data under the Agreement including (without limitation) the GDPR, the UK GDPR, and the CCPA, as applicable to the Processing of Personal Data hereunder**.**
Data Protection Losses	means all losses and liabilities, including all: (i) costs (including legal costs), claims, demands, actions, settlements, interest, charges, expenses, losses and damages; (ii) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (iii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; (iv) the reasonable costs of compliance with investigations by a Supervisory Authority; (v) costs of investigation including forensic investigation; (vi) cost of breach notification including notifications to the Data Subjects; and (vii) cost of complaints handling including providing Data Subjects with credit reference checks, setting up contact centres (e.g. call centres), producing end customer communication materials, provision of insurance to end customers (e.g. identity theft), and reimbursement of costs incurred by end customers (e.g. changing locks);
Data Subject	means the identified or identifiable person to whom Personal Data relates;
Data Subject Request	means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;
EU GDPR **GDPR**	means the General Data Protection Regulation (EU) 2016/679; means as applicable the UK GDPR or the EU GDPR
International Recipient	has the meaning given to that term in clause 8.1;
Personal Data	means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws);

Personal Data Breach	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;
Processor	means the entity which Processes Personal Data on behalf of the Controller;
processing	means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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, restriction, erasure or destruction (and related terms such as **process** have corresponding meanings);
Processing Instructions	has the meaning given to that term in clause 4.2(b);
Protected Data	means Personal Data provided to Commonplace by the Customer, or otherwise received by Commonplace in connection with the provision of the Services (including responses from and information about community users on the Commonplace Platform), pursuant to the Services Agreement;
Services	means the services provided to Customer by Commonplace pursuant to the Services Agreement;
Shared Personal Data	has the meaning given in clause 2.3.
Sub-Processor	means another Processor engaged by Commonplace for carrying out processing activities in respect of the Protected Data on behalf of Commonplace;
Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;
UK GDPR	UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit)_Regulations 2019 (DPPEC Regulations).
Working Day	means Monday to Friday inclusive excluding bank and public holidays in the UK.

2. **Roles And Obligations**

2.1 The parties agree that, for the Protected Data, Customer shall be the Controller and Commonplace shall be the Processor. For the purposes of the CCPA (and to the extent applicable), Customer is the "Business" and Commonplace is the "Service Provider".

2.2 Commonplace shall process the Protected Data in compliance with:

(a) the obligations of Processors under Data Protection Laws and so as not to place Customer in breach of Customer's obligations as a Controller of that Protected Data in the country where the processing takes place; and
(b) the terms of this DPA.

2.3 The parties acknowledge that Commonplace also uses some of the Protected Data collected via the Commonplace Platform for its own purposes, as set out in the Commonplace Privacy Policy. This is considered to be "Shared Personal Data" in respect of which the parties are independent Controllers. Further provisions relating to how the parties process such Shared Personal Data are set out in Appendix 2.

3. **Customer Obligations**

3.1 Customer shall, in its use of the Services, Process Protected Data in accordance with the requirements of Data Protection Laws. Customer shall ensure all Protected Data it provides to Commonplace for use in connection with the Services, or that it requests Commonplace to collect via the Services, shall be collected and/or transferred to Commonplace in accordance with Data Protection Laws.

3.2 It shall be Customer's responsibility to: (i) ensure the terms of use it supplies to the Data Subjects of the Protected Data comply with Data Protection Laws including in particular any fair processing information requirements relating to the processing of the Protected Data by Commonplace and (ii) ensure it has a legal basis for the processing of the Protected Data by Commonplace. To that end Customer shall ensure that it provides copies of its privacy policy and other fair processing notices for Commonplace to post on the Customer-initiated Commonplace Platform and Customer shall ensure that where it requires Special Category Data to be collected that it has: (i) identified the purpose for which such processing is necessary; (ii) checked that the processing of the special category data is necessary for that purpose and that it has identified and is satisfied there is no other reasonable and less intrusive way to achieve that purpose; and (iii) identified an Article 6 GDPR lawful basis and an appropriate Article 9 GDPR condition, for processing the special category data.

4. **Instructions**

4.1 Customer's instructions for the Processing of Protected Data shall comply with Data Protection Laws.

4.2 Commonplace:

(a) shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with Customer's documented lawful instructions from time to time and as permitted within the parameters of the Services; and
(b) in accordance with Appendix 1 (Data Processing Particulars), as updated from time to time by written agreement of the parties or as otherwise detailed in the Agreement ("**Processing Instructions"**); and
(c) shall inform Customer if Commonplace is aware of a Processing Instruction that, in its opinion, infringes Data Protection Laws.

5. **Technical and Organisational Measures**

5.1 Commonplace shall implement and maintain:

(a) the technical and organisational measures prescribed by Data Protection Laws; and
(b) taking into account the nature of the processing, the technical and organisational measures necessary to assist Customer insofar as is reasonably possible in the fulfilment of Customer's obligations to respond to Data Subject Requests relating to Protected Data.

6. **Sub Processors and Staff**

6.1 Commonplace has appointed those Sub-Processor(s) listed in Appendix 1 to this DPA under a written contract containing materially equivalent obligations to those in this DPA. Commonplace shall provide Customer with a copy of the agreements with Sub-Processors if requested to do so by Customer. Commonplace may redact commercial terms from such agreements before disclosing them to Customer.

6.2 Commonplace shall ensure that all of its personnel and contractors processing Protected Data are subject to a binding written contractual obligation with Commonplace or under professional obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case Commonplace shall, where practicable and not prohibited by Applicable Law, notify Customer of any such requirement before such disclosure).

6.3 Commonplace will maintain a list of Sub-Processors and will notify Customer by email (to Customer Contact – Legal and Data Protection) of any new Sub-Processors. If Customer has a reasonable objection to any new Sub-Processor, it will notify Commonplace of such objection in writing within ten days of receiving the email notification and the parties will seek to resolve the matter in good faith.

6.4 If Commonplace can provide the Services to Customer in accordance with the Services Agreement without using the Sub-Processor and decides in its discretion to do so, then Customer will have no further rights in respect of the proposed Sub-Processor. If Commonplace requires the Sub-Processor and is unable to satisfy Customer as to the suitability of the Sub-Processor or the documentation in place between Commonplace and the Sub-Processor within 30 days from Customer's notification of objections, Customer may within 20 days of the end of the 30-day period referred to above terminate the Services Agreement [only in relation to the Services to which the proposed new Sub-Processor's processing of Protected Data would relate] by providing written notice to Commonplace.

7. **Data Subject Request Assistance**

7.1 Commonplace shall promptly refer all Data Subject Requests it receives to Customer (wherever practicable within two Working Days of receipt of the request).

7.2 Commonplace shall provide such assistance to Customer as Customer reasonably requires (taking into account the nature of processing and the information available to Commonplace) to ensure compliance with each party's obligations under Data Protection Laws with respect to:

(a) Data Subject Requests;
(b) security of processing;
(c) data protection impact assessments (as such term is defined in Data Protection Laws);
(d) prior consultation with a Supervisory Authority regarding high risk processing; and
(e) notifications to the Supervisory Authority and/or communications to Data Subjects by Customer in response to any Personal Data Breach and for the avoidance of doubt Commonplace must promptly notify Customer in writing of any communications received by it from Data Subjects or Supervisory Authorities relating to the Protected Data without responding to either of the same unless it has been expressly authorised to do so by Customer.

8. **Overseas Transfers**

8.1 **Transfers from the EEA, Switzerland and the United Kingdom to countries that offer adequate level or data protection**. Personal Data may be transferred from EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**"), Switzerland and the United Kingdom ("**UK**") to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the Member States or the European Commission, Switzerland, and/or the UK as relevant ("**Adequacy Decisions**"), as applicable, without any further safeguard being necessary.

8.2 **Transfers from the EEA, Switzerland and the United Kingdom to other countries**. If the Processing of Personal Data by Processor includes a transfer (either directly or via onward transfer):

(a) from the EEA or Switzerland to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Processor for the lawful transfer of personal data (as defined in the GDPR) outside the EEA or Switzerland ("**EEA Transfer**"), the terms set forth in Part 1 of **Schedule 2** (EEA Cross Border Transfers) shall apply;

(b) from the UK to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Processor for the lawful transfer of personal data (as defined in the UK GDPR) outside the EEA or UK ("**UK Transfer**"), the terms set forth in Part 2 of **Schedule 2** (UK Cross Border Transfers) shall apply;

(c) the terms set forth in Part 3 of **Schedule 2** (Additional Safeguards) shall apply to an EEA Transfer and a UK Transfer.

9. Records and Audits

9.1 Commonplace shall maintain written records of all categories of processing activities carried out on behalf of Customer.

9.2 Commonplace shall make available to Customer such information as is reasonably necessary to demonstrate its compliance with the obligations of Processors under Data Protection Laws, and shall allow for and contribute to audits, including inspections, by Customer (or another auditor mandated by Customer) for this purpose, subject to Customer:

(a) not requesting an audit or inspection more than once in each twelve-month period (unless there has been an actual or suspected Personal Data Breach);
(b) giving Commonplace at least 30 days' advance notice of such information request, audit and/or inspection being required; and
(c) Customer and Commonplace mutually agreeing the scope, timing, and duration of the audit and any reimbursement of Commonplace's costs in facilitating audits and inspections; and
(d) ensuring that all information obtained or generated by Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law). Customer shall provide a copy of such information and audit reports to Commonplace following an inspection or audit pursuant to this clause 9.

(e) Customer shall return all records or documentation in Customer's possession or control provided by Processor in the context of the audit and/or the inspection). If and to the extent that the Standard Contractual Clauses apply, nothing in this Section 9.2 varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

9.3 In the event of an audit or inspections as set forth above, Customer shall ensure that it (and each of its mandated auditors) will not cause (or, if it cannot avoid, minimize) any damage, injury or disruption to Processor's premises, equipment, personnel and business while conducting such audit or inspection.

9.4 The audit rights set forth in 9.2 above, shall only apply to the extent that the Agreement does not otherwise provide Customer with audit rights that meet the relevant requirements of Data Protection Laws (including, where applicable, article 28(3)(h) of the GDPR or the UK GDPR).

10. Breach Notification

10.1 In respect of any Personal Data Breach involving Protected Data, Commonplace shall without undue delay of becoming aware of the Personal Data Breach:

(a) notify Customer of the Personal Data Breach; and
(b) so far as possible without prejudicing the continued security of the Protected Data or any investigation into the Personal Data Breach, provide Customer with details of the Personal Data Breach.

10.2 Processor shall make reasonable efforts to identify and take those steps as Processor deems necessary and reasonable in order to remediate the cause of such Data Incident to the extent the remediation is within Processor's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or anyone who uses the Services on Customer's behalf. Customer will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Data Incident which directly or indirectly identifies Processor (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Processor's prior written approval, unless, and solely to the extent that, Customer is compelled to do so pursuant to applicable Data Protection Laws. In the latter case, unless prohibited by law, Customer shall provide Processor with reasonable prior written notice to provide Processor with the opportunity to object to such disclosure and in any case Customer will limit the disclosure to the minimum scope required.

11. Deletion or Return of Data

11.1 Without prejudice to clauses 11.2 and subject to the provisions of Appendix 2 in relation to Shared Personal Data and any storage requirements under Applicable Law, Commonplace shall either delete, return all the Protected Data to Customer or put the Protected Data beyond use as soon as reasonably practicable following the end of:

(a) the provision of the relevant Services related to processing of that data; or

(b) the Archive Period as set out on the Order Form.

11.2 Customer agrees that Commonplace may anonymise a copy of Protected Data (to the extent it has not already been anonymised prior to termination) and Commonplace may use such anonymised Protected Data for its own business purposes including making improvements to its Services generally and for improving engagement with communities and other customers.

12. Indemnity and Liability

12.1 Each party ("**Indemnifying Party**") shall indemnify and keep indemnified the other ("Indemnified Party") in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, the Indemnified Party arising from or in connection with any:

(a) non-compliance by the Indemnifying Party with the Data Protection Laws; and
(b) breach by the Indemnifying Party of any of its obligations under this DPA.

12.2 If a party receives a compensation claim from a person (including but not limited to a Data Subject) relating to processing of Protected Data processed by Commonplace under this Agreement, it shall promptly provide the other party with notice and full details of such claim. Commonplace shall make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of Customer.

12.3 As between Commonplace and the Customer liability for all Data Protection Losses arising out of any breach of this DPA including for any loss or damage arising out of a Personal Data Breach, shall be subject to the limits of liability set out in the Services Agreement.

13. Change in Law

Notwithstanding anything to the contrary in this DPA, in the event: (i) of a change in any law or regulation or (ii) a regulator issues a binding instruction, order or requirement which changes the basis on which the Protected Data can be processed, transferred or stored pursuant to this DPA, the parties agree to negotiate in good faith to agree an amendment to this DPA and the Services Agreement (to the extent necessary) to address such change in law or regulation or to comply with a binding instruction, order or requirement as applicable.

SCHEDULE 1: APPENDIX 1
DATA PROCESSING PARTICULARS

[Detail to be reviewed and updated for each customer]

1. **Subject-matter of processing:**
   a) Collecting and analysing public feedback using the Commonplace Platforms for the purposes of the Project Services and also: Providing the Services to Customer;
   b) Performing the Agreement, this DPA and/or other contracts executed by the Parties;
   c) Acting upon Customer's instructions, where such instructions are consistent with the terms of the Agreement;
   d) Sharing Personal Data with third parties in accordance with Customer's instructions and/or pursuant to Customer's use of the Services (e.g., integrations between the Services and any services provided by third parties, as configured by or on behalf of Customer to facilitate the sharing of Personal Data between the Services and such third-party services);
   e) Complying with applicable laws and regulations;
   f) All tasks related with any of the above.

2. **Duration of the processing:**

   Subject to Clause 11 of this DPA, Commonplace will Process Protected Data for the duration of the provision of the Services, unless otherwise agreed upon in writing.

3. **Nature and purpose of the processing:**

   To use the Protected Data for the purpose of providing the Services and as otherwise detailed in the Services Agreement, and as further instructed by Customer in its use of the Services.

4. **Type of Personal Data:**

   Using the configuration options on the Commonplace Platform the Customer determines and controls the type of Protected Data to be collected via the Commonplace Platform for its (and its Project Partners') purposes which may include, but is not limited to the following categories of Personal Data:

   - First and last name
   - Contact information (email, physical address)
   - Professional life data
   - Personal life data
   - Connection data (e.g. IP address)
   - Localisation data
   - Demographic data (e.g. post code)
   - Free text comments (retained for the Customer separately from but linkable with, Data Subject identifiers).
   - City hotline / help service information (e.g. in the USA, 311 reports) - full name, address and contact information such as mobile phone number and email address, demographic information such as location, contact details and details regarding the content of the report (location, subject matter and additional information provided by the Resident).
   - Social media activity - name, social media handle (which is later hashed), content uploaded to social media platform (e.g. posts, comments, interactions and tweets from Facebook, Twitter, Instagram and NextDoor, both if made publicly available on the relevant platform or if contained in a group to which Commonplace is granted access.
   - Community Surveys – name, email address, telephone number, address, and answers to survey questions.
   - City hotlines information (e.g. 311 reports), social media activity and community surveys – Name and other identifying information which is provided by Residents and contained in any Resident Data referred to in (i) above.
   - Name and other identifying information contained in news publications and broadcast media (e.g. online news websites, public forums, etc).

   Special Category Data:

   - race;
   - ethnic origin;
   - politics;
   - religion;
   - health;

5. Categories of Data Subjects:

Using the configuration options on the Commonplace Platform the Customer determines and controls the categories of Data Subjects from which Protected Data is collected via the Commonplace Platform for its (and its Project Partners') purposes:

- Individuals in a community that engage in the Commonplace Platform.
- Individuals who engage with municipal services such as resident requests submitted to city hotlines (e.g. 311 services), social-media activity involving the municipality or local council (e.g. posts, comments, interactions and tweets from different social media platforms such as Facebook, Twitter, Instagram and NextDoor), and community surveys ("**Resident(s)**");
- Individuals referred to within Resident Data (for example, if a Resident posts about their mayor on social media, the information relating to the mayor) or local media reports ("**Referred Individual(s)**");

6. Processing Instructions

Using the configuration and set up options on the Commonplace Platform, the Customer determines and controls how the Protected Data is collected and processed via the Commonplace Platform.

Commonplace is generally instructed to use the Protected Data for the purpose of providing the Services as configured by the Customer and as otherwise detailed in the Services Agreement.

7. Sub-Processors

Commonplace uses sub-processors, which are providers that support its platform. The complete list of sub-processors and their function can be foun

SCHEDULE 1: APPENDIX 2

Controller Terms

1. **Parties' obligations relating to Shared Personal Data.**

1.1 In respect of the Shared Personal Data:

1.1.1 the parties acknowledge and agree that each party shall be Controller in its own right. Each party will comply with the Data Protection Laws and will not do any act or make any omission which puts the other party in breach of its obligations under the Data Protection Laws; and

1.1.2 the parties agree to provide reasonable assistance as is necessary to each other to comply with its obligations under the Data Protection Laws, including:

:

(a) consulting with the other party about any notices given to, and/or consents received from, Data Subjects in relation to the Shared Personal Data;
(b) promptly informing the other party about the receipt of any Data Subject Requests;
(c) providing the other party with reasonable assistance in complying with any Data Subject Requests;
(d) facilitating the handling of any Personal Data Breach for which the other party is responsible as soon as reasonably practicable upon becoming aware, which shall include the party responsible for the breach notifying the relevant Supervisory Authority, promptly and in any event no later than 72 hours after becoming aware of it, as well as the relevant Data Subjects without undue delay, where required by the Data Protection Laws;
request without first consulting the
(e) responding within a reasonable time to any enquiries from a Supervisory Authority; and
(f) notifying the other party without undue delay on becoming aware of any breach of the Data Protection Laws.

2. **Restrictions on use**

The Disclosing Party discloses Personal Data to the Receiving Party solely for the purposes permitted by the Agreement. The Receiving Party will not “Sell” or “Share” (as both terms are defined in applicable Data Protection Laws) Personal Data provided by Counterparty pursuant to the Agreement, or otherwise retain, use, disclose, or process Personal Data, for any purpose other than for the specific purposes set forth herein or otherwise outside the direct business relationship between the parties. The Receiving Party will comply with all applicable requirements of applicable Data Protection Law, including but not limited to by: (i) providing the same level of privacy protection to Personal Data as required the Disclosing Party under applicable Data Protection Law, and in no event less than a reasonable standard of care; (ii) providing any required disclosures, such as privacy policies, notices at collection, or opt out notices to consumers whose Personal Data the Receiving Party processes; and (iii) implementing appropriate technical and organizational measures to ensure a level of security for the Personal Data appropriate to the risk. The Disclosing Party shall have the right, upon reasonable notice to the Receiving Party, to take reasonable and appropriate steps to help ensure that the Receiving Party uses the Personal Data transferred in a manner consistent with Data Protection Laws and to stop and remediate unauthorized use of Personal Data. The Receiving Party shall notify the Disclosing Party if it makes a determination that it can no longer meet its obligations under this Addendum and in such case each Party shall be entitled to terminate the Agreement..

3. Indemnity.

Each party shall indemnify the other against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred by the indemnified party arising out of or in connection with the breach of this Appendix 2 affecting Shared Personal Data, provided that the indemnified party gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend and/or settle it. The liability of the indemnifying party under this clause shall be subject to the limits of liability set out in the Services Agreement.

SCHEDULE 2 - Cross Border Transfers

PART 1 – EEA Transfers

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to an EEA Transfer.
2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Customer as the data controller of the Personal Data and Commonplace is the data processor of the Personal Data.
3. Clause 7 of the Standard Contractual Clauses (Docking Clause) shall not apply.
4. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the Standard Contractual Clauses shall apply, and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in Section 5.2 of the DPA.
5. In Clause 11 of the Standard Contractual Clauses, the optional language will not apply.
6. In Clause 17 of the Standard Contractual Clauses, Option 1 shall apply, and the Parties agree that the Standard Contractual Clauses shall be governed by the laws of the England and Wales.
7. In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of England and Wales.
8. Annex I.A of the Standard Contractual Clauses shall be completed as follows:

   Data Exporter: Customer.

   Contact details: As detailed in the Agreement.

   Data Exporter Role: The Data Exporter is a data controller.

   Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

   Data Importer: Commonplace Technologies Ltd.

   Contact details: As detailed in the Agreement.

   Data Importer Role: The Data Importer is a data processor.

   Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

9. Annex I.B of the Standard Contractual Clauses shall be completed as follows:

   The categories of data subjects are described in Schedule 1 (Details of Processing) of this DPA.

   The categories of personal data are described in Schedule 1 (Details of Processing) of this DPA.

   The Parties do not intend for Sensitive Data to be transferred.

   The frequency of the transfer is a continuous basis for the duration of the Agreement.

   The nature of the processing is described in Schedule 1 (Details of Processing) of this DPA.

   The purpose of the processing is described in Schedule 1 (Details of Processing) of this DPA.

   The period for which the personal data will be retained is for the duration of the Agreement, unless agreed otherwise in the Agreement and/or the DPA.

   In relation to transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth at the link detailed in Section 5.2.1 of the DPA.

10. Annex I.C of the Standard Contractual Clauses shall be completed as follows:

    The competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 7 above.

11. The Security Documentation referred to in the DPA serves as Annex II of the Standard Contractual Clauses.
12. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses will prevail.

PART 2 – UK Transfers

1. This Part 2 is effective from the same date as the Standard Contractual Clauses.

Background:

2. This Part 2 is intended to provide appropriate safeguards for the purposes of transfers of Personal Data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.

Interpretation:

3. Where this Part 2 uses terms that are defined in the Standard Contractual Clauses, those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland

4. This Part 2 shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.
5. This Part 2 shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this DPA has been entered into.
7. In the event of a conflict or inconsistency between this Part 2 and the provisions of the Standard Contractual Clauses or other related agreements between the Parties, existing at the time the DPA is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.
8. This Part 2 incorporates the Standard Contractual Clauses which are deemed to be amended to the extent necessary so they operate:

   a. for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and

   b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 8 above, include (without limitation):
   a. References to the "Clauses" means this Part 2 as it incorporates the Standard Contractual Clauses
   b. Clause 6 Description of the transfer(s) is replaced with:

      "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."

   c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.
   d. References to Regulation (EU) 2018/1725 are removed.
   e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"
   f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;
   g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".
   h. Clause 18 is replaced to state:

      "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."

i. The footnotes to the Clauses do not form part of this Part 2.

10. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.
11. The Parties may amend this Part 2 provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Standard Contractual Clauses and making changes to them in accordance with Section 8 above.
12. The Parties may give force to this Part 2 (incorporating the Standard Contractual Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Contractual Clauses.

PART 3 – Additional Safeguards

1. In the event of an EEA Transfer or a UK Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:
    a. The Processor shall have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from the Controller to the Processor and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of personal data whilst in transit and at rest intended to deny attackers the ability to read data.
    b. The Processor will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the personal data protected under GDPR or the UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Court ("**FISA**");
    c. If the Processor becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:
        i. The Processor shall inform the relevant government authority that the Processor is a processor of the Personal Data and that the Controller has not authorized the Processor to disclose the Personal Data to the government authority, and inform the relevant government authority that any and all requests or demands for access to personal data should therefore be notified to or served upon the Controller in writing;
        ii. The Processor will use commercially reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under the Processor's control. Notwithstanding the above, (a) the Controller acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) if, taking into account the nature, scope, context and purposes of the intended government authority access to Personal Data, the Processor has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, this subsection (e)(II) shall not apply. In such event, the Processor shall notify the Controller, as soon as possible, following the access by the government authority, and provide the Controller with relevant details of the same, unless and to the extent legally prohibited to do so.

2. Once in every 12-month period, the Processor will inform the Controller, at the Controller's written request, of the types of binding legal demands for Personal Data it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.

SCHEDULE 3: PAUSE FEES

After the end date (and hence expiry) of any licence, all projects associated with that licence will be closed, such that edit mode and dashboard are inaccessible

A closed project or hub cannot be reactivated after the expiration of the licence (or a continuous renewal of said licence) to which the project was associated

In certain circumstances, and entirely at the discretion of Commonplace, one of the following options may be offered to customers who are unable to renew the license:

1. Licence pause (Project £200 per month, Departmental £300 per month, Corporate £600 per month - minimum 6 months) - projects associated with the licence will be paused for engagement & news purposes (no access to edit mode), but the dashboard & exports can still be accessed in order to continue with analysis and evaluation (any add-ons such as TrendsAI, PDF Clipper, Embeddable Charts are disactivated)

2. Licence suspension (Project £100 per month, Departmental £150 per month, Corporate £300 per month - minimum 6 months) - all projects associated with the licence will be closed (no access to edit mode or dashboard), but can be reactivated at a future date after which the licence has been reactivated

Additional closure costs (not for GCloud)	**Before expiration of licence**	**During pause / suspension**	**After expiration of licence**
URL deletion request (requires approval by Commonplace data protection manager)	£250 / URL	£250 / URL	£500 / URL
URL renaming / redirect request	£250 / URL	£250 / URL	£500 / URL
Hide URL from search engines (requires approval by Commonplace data protection manager)	£250 / URL	£250 / URL	£500 / URL
Maintenance of custom domain	NA	£250 / URL / yr	£250 / URL / yr
Substantial administrative requests of the support team not associated to project build or evaluation (eg. editing / content download / screenshots / providing list of admins)	£150 / hr	£150 / hr	£150 / hr
Data exports	Included	Included for pause £2 / contribution or respondent or user for suspension up to max £10k	£2 / contribution or respondent or user up to max £10k
Report writing / analysis (not incl TrendsAI)	See add-ons	See add-ons	£250 / hr
Request by customer to delete contribution (decision will rest with our data protection manager)	£25 per contribution	£25 per contribution	£50 per contribution