

COMMON SENSE MEDIA UK DIGITAL CITIZENSHIP DPA

THIS DATA PROCESSING ADDENDUM is entered into as of the Addendum Effective Date by and between: (1) Common Sense Media, Inc., whose ordinary business address is at 699 8th Street, Suite C150, San Francisco, California 94103, USA (“**CSM**”); and (2) the UK-based Educational Institution registered to use the Digital Citizenship Offering under and pursuant to the Terms of Service (the “**UK Educational Institution**”).

1. INTERPRETATION AND APPLICATION

1.1. In this Data Processing Addendum the following terms shall have the meanings set out in this Paragraph 1.1, unless expressly stated otherwise:

- (a) “**Addendum Effective Date**” means the date on which the UK Educational Institution first Makes Available an Institution Input on or via the Digital Citizenship Offering.
- (b) “**Cessation Date**” has the meaning given in Paragraph 9.1.
- (c) “**Data Protection Laws**” means the UK GDPR, the Data Protection Act 2018 and any other applicable law relating to data protection or data privacy.
- (d) “**Data Subject Request**” means the exercise by Data Subjects of their rights under, and in accordance with, Chapter III of the UK GDPR.
- (e) “**Data Subject**” means the identified or identifiable natural person to whom Institution Personal Data relates.
- (f) “**ICO**” means the UK Information Commissioner’s Office.
- (g) “**Institution Personal Data**” means any Personal Data comprised within Institution Inputs, which is Processed by CSM for and on behalf of the UK Educational Institution as a Processor for the purpose of providing the Services.
- (h) “**Personnel**” means a person’s employees, agents, consultants or contractors.
- (i) “**Restricted Transfer**” means the transmission of Personal Data to a person in a country or territory outside the UK, which the UK Government has not deemed to provide an ‘adequate’ level of protection for Personal Data pursuant to a decision made or approved under Article 45 of the UK GDPR.
- (j) “**Services**” means those services to be supplied to or carried out by or on behalf of CSM for the UK Educational Institution via the Digital Citizenship Offering pursuant to the Terms of Service.
- (k) “**Standard Contractual Clauses**” means the standard contractual clauses issued or approved from time-to-time by the UK Government or the ICO under Article 46 of the UK GDPR for use in respect of Restricted Transfers from Controllers to Processors – the current form of which is attached hereto as Annex 4.
- (l) “**Subprocessor**” means any third party appointed by or on behalf of CSM to Process Institution Personal Data.
- (m) “**Terms of Service**” means the *Common Sense Media – UK Digital Citizenship Terms of Service* posted at

<https://www.common sense media.org/about-us/our-mission/uk-digital-citizenship-terms-of-service> (or any successor page or site) from time to time.

- (n) **“UK GDPR”** means the EU General Data Protection Regulation 2016/679 as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019).

1.2. In this Data Processing Addendum:

- (a) the terms, **“Controller”**, **“Processor”**, **“Personal Data”**, **“Personal Data Breach”** and **“Process”** (and its inflections) shall have the meaning ascribed to the corresponding terms in the UK GDPR;
- (b) unless otherwise defined in this Data Processing Addendum, all capitalised terms used herein (including the pre-amble above) shall have the meaning given to them in the Terms of Service.

2. PROCESSING OF INSTITUTION PERSONAL DATA

2.1. In respect of Institution Personal Data, the Parties acknowledge that, as between the Parties:

- (a) CSM is engaged to act as a Processor; and
- (b) the UK Educational Institution acts as the Controller.

2.2. CSM shall:

- (a) comply with applicable Data Protection Laws in Processing Institution Personal Data; and
- (b) not Process Institution Personal Data other than:
 - (i) on the UK Educational Institution’s instructions (subject always to Paragraph 2.8); and
 - (ii) as required by applicable laws.

2.3. To the extent permitted by applicable laws, CSM shall inform the UK Educational Institution of:

- (a) any Processing to be carried out under Paragraph 2.2(b)(ii); and
- (b) the relevant legal requirements that require it to carry out such Processing, before the relevant Processing of that Institution Personal Data.

2.4. The UK Educational Institution instructs CSM to Process Institution Personal Data as necessary:

- (a) to provide the Services to the UK Educational Institution; and
- (b) to perform CSM’s obligations and exercise CSM’s rights under the Terms of Service.

2.5. Annex 1 (*Data Processing Details*) sets out certain information regarding CSM’s Processing of Institution Personal Data as required by Article 28(3) of the UK GDPR.

- 2.6. Nothing in Annex 1 (*Data Processing Details*) (including as amended pursuant to Paragraph 2.6) confers any right or imposes any obligation on any Party to this Data Processing Addendum.
- 2.7. Where CSM receives an instruction from the UK Educational Institution that, in its reasonable opinion, infringes the UK GDPR, CSM shall inform the UK Educational Institution.
- 2.8. The UK Educational Institution acknowledges and agrees that any instructions issued by the UK Educational Institution with regards to the Processing of Institution Personal Data by or on behalf of CSM pursuant to or in connection with the Terms of Service:
- (a) shall be strictly required for the sole purpose of ensuring compliance with Data Protection Laws;
 - (b) shall not relate to the scope of, or otherwise materially change, the Services to be provided by CSM under the Terms of Service; and
 - (c) unless otherwise agreed between the Parties shall be communicated by the UK Educational Institution to CSM by email to compliance@commonsense.org.
- 2.9. Notwithstanding anything to the contrary herein, CSM may terminate the agreement formed between the Parties under the Terms of Service in its entirety upon written notice to the UK Educational Institution with immediate effect if CSM considers (in its reasonable discretion) that:
- (a) it is unable to adhere to, perform or implement any instructions issued by the UK Educational Institution (including as a result of the technical limitations of its systems, equipment and/or facilities); and/or
 - (b) to adhere to, perform or implement any such instructions would require disproportionate effort (whether in terms of time, cost, available technology, manpower or otherwise).
- 2.10. The UK Educational Institution represents and warrants on an ongoing basis that, for the purposes of Article 6 of the UK GDPR (as supplemented by Article 8 of the UK GDPR where relevant), and (where applicable) Article 9 and/or Article 10 of the UK GDPR, there is, and will be throughout the term of the Terms of Service, a valid legal basis for the Processing by CSM of Institution Personal Data in accordance with this Data Processing Addendum and the Terms of Service (including, any and all instructions issued by the UK Educational Institution from time to time in respect of such Processing).
- 2.11. UK Educational Institution represents and warrants on an ongoing basis that it has entered into and shall maintain an agreement with the provider of any Education Platform, which:
- (a) to the fullest extent required permits CSM to access certain Institution Personal Data from the Education Platform as contemplated by Annex 1 (*Data Processing Details*) or otherwise as necessary to provide the Digital Citizenship Offering; and
 - (b) incorporates a valid data processing addendum, which conforms to the requirements of Article 28(3) of the UK GDPR (including Standard Contractual Clauses if and as applicable).

3. CSM PERSONNEL

CSM shall take reasonable steps to ensure the reliability of any CSM Personnel who Process Institution Personal Data, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. SECURITY

- 4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk (which may be of varying likelihood and severity) for the rights and freedoms of natural persons, CSM shall in relation to Institution Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the UK GDPR.
- 4.2. In assessing the appropriate level of security, CSM shall take account in particular of the risks presented by the Processing, in particular from a Personal Data Breach.
- 4.3. Without limiting the generality of Paragraphs 4.1 and 4.2, CSM shall endeavour to comply with the security measures set out in Annex 3.

5. SUBPROCESSING

- 5.1. The UK Educational Institution authorises CSM to appoint Subprocessors in accordance with this Paragraph 5.
- 5.2. CSM may continue to use those Subprocessors already engaged by CSM as at the date of this Data Processing Addendum (a list of whom is set out in Annex 2 (*Subprocessors*)).
- 5.3. CSM shall give the UK Educational Institution prior written notice of the appointment of any new Subprocessor – which may be given by way of CSM posting an updated form of Annex 2 (*Subprocessors*). If, within five (5) business days of receipt of that notice, the UK Educational Institution notifies CSM in writing of any objections (on reasonable grounds) to the proposed appointment:
 - (a) CSM may, but shall not be obliged to, elect to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and
 - (b) where:
 - (i) such a change cannot be made within fifteen (15) business days from CSM receipt of the UK Educational Institution's notice;
 - (ii) no commercially reasonable change is available or CSM elects not to make any such change; and/or

(iii) the UK Educational Institution declines to bear the cost of the proposed change,

either Party may by written notice to the other Party with immediate effect terminate the agreement formed between the Parties under the Terms of Service and, for the avoidance of doubt, the UK Educational Institution shall cease all use of the Digital Citizenship Offering.

- 5.4. With respect to each Subprocessor, CSM shall ensure that the arrangement between CSM and the Subprocessor is governed by a written contract including terms which offer at least an equivalent level of protection for Institution Personal Data as those set out in this Data Processing Addendum.
- 5.5. The UK Educational Institution acknowledges and agrees that the provider of Education Platform acts as its direct Processor, and does not constitute a Subprocessor acting on behalf of CSM.

6. DATA SUBJECT RIGHTS

- 6.1. Taking into account the nature of the Processing, CSM shall provide the UK Educational Institution with such assistance as may be reasonably necessary and technically possible in the circumstances, to assist the UK Educational Institution in fulfilling its obligation to respond to Data Subject Requests.
- 6.2. CSM shall:
- (a) promptly notify the UK Educational Institution upon becoming aware that it has received a Data Subject Request in respect of Institution Personal Data; and
 - (b) ensure that CSM does not respond to any Data Subject Request except on the written instructions of the UK Educational Institution (and in such circumstances, at the UK Educational Institution's cost) or as required by applicable laws.

7. PERSONAL DATA BREACH

- 7.1. CSM shall notify the UK Educational Institution without undue delay upon CSM becoming aware of a Personal Data Breach affecting Institution Personal Data, providing the UK Educational Institution with sufficient information (insofar as such information is, at such time, within CSM's possession) to allow the UK Educational Institution to meet any obligations under Data Protection Laws to report the Personal Data Breach to:
- (a) affected Data Subjects; and
 - (b) the ICO.
- 7.2. CSM shall at the UK Educational Institution's sole cost and expense co-operate with the UK Educational Institution and take such reasonable commercial steps as may be directed by the UK Educational Institution to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

CSM shall provide reasonable assistance to the UK Educational Institution, at the UK Educational Institution's cost, with any data protection impact assessments, and prior consultations with the

ICO, which the UK Educational Institution reasonably considers to be required of the UK Educational Institution by Article 35 or Article 36 of the UK GDPR, in each case solely in relation to Processing of Institution Personal Data by, and taking into account the nature of the Processing by, and information available to, CSM.

9. **DELETION**

- 9.1. Upon the date of cessation of the Services (the “**Cessation Date**”), CSM shall cease all Processing of the Institution Personal Data for any purpose other than for storage.
- 9.2. The UK Educational Institution may within ten (10) business days of the Cessation Date request that CSM:
 - (a) return a copy of all Institution Personal Data then-held by CSM to the UK Educational Institution by secure file transfer in a reasonably interoperable format; or
 - (b) delete all Institution Personal Data then-held by CSM.
- 9.3. Promptly following the return Institution Personal Data pursuant to a request made under Paragraph 9.2(a), CSM shall delete all other copies of Institution Personal Data then-held by CSM.
- 9.4. In the event that the UK Educational Institution does not make a request for return or deletion under, and within the timeframe set out in, Paragraph 9.2, CSM shall promptly delete all Institution Personal Data then-held by CSM.
- 9.5. Notwithstanding anything to the contrary in the foregoing, CSM may retain Institution Personal Data to the extent required by applicable law, and only to the extent and for such period as required by applicable law, provided that CSM shall ensure:
 - (a) the confidentiality of all such Institution Personal Data; and
 - (b) that such Institution Personal Data is only Processed as necessary for the purpose(s) specified in the applicable law requiring its retention and for no other purpose.

10. **AUDIT RIGHTS**

- 10.1. CSM shall make available to the UK Educational Institution on request such information as CSM (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this Data Processing Addendum.
- 10.2. Subject to Paragraphs 10.3 and 10.4, in the event that the UK Educational Institution (acting reasonably) is able to provide documentary evidence that the information made available by CSM pursuant to Paragraph 10.1 is not sufficient in the circumstances to demonstrate CSM's compliance with this Data Processing Addendum, CSM shall allow for and contribute to audits, including on-premise inspections, by the UK Educational Institution or an auditor mandated by the UK Educational Institution in relation to the Processing of the Institution Personal Data by CSM.

- 10.3. The UK Educational Institution shall:
- (a) give CSM reasonable notice of any audit or inspection to be conducted under Paragraph 10.1 (which shall in no event be less than ten (10) business days' notice, unless a shorter period is mandated by the ICO pursuant to Paragraph 10.4(f)); and
 - (b) use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing, and hereby indemnifies CSM in respect of, any damage, injury or disruption to CSM's premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of CSM's other users/customers or the availability of CSM's services to such other users/customers) while its Personnel and/or its auditor's Personnel (if applicable) are on those premises in the course of any on-premise inspection.
- 10.4. CSM need not give access to its premises for the purposes of such an audit or inspection:
- (a) to any individual unless he or she produces reasonable evidence of their identity and authority;
 - (b) to any auditor whom CSM has not given its prior written approval (not to be unreasonably withheld);
 - (c) unless the auditor enters into a non-disclosure agreement with CSM on terms acceptable to CSM;
 - (d) where, and to the extent that, CSM considers, acting reasonably, that to do so would result in interference with the confidentiality or security of the data of CSM's other users/customers or the availability of CSM's services to such other users/customers;
 - (e) outside normal business hours at those premises; or
 - (f) on more than one occasion in any calendar year during the term of the Terms of Service, except for any additional audits or inspections which the UK Educational Institution is required to carry out by Data Protection Laws and/or the ICO, where the UK Educational Institution has identified the relevant requirement in its notice to CSM of the audit or inspection.
- 10.5. The UK Educational Institution shall bear any third party costs in connection with such inspection or audit and reimburse CSM for all costs incurred by CSM and time spent by CSM (at CSM's then-current rates) in connection with any such inspection or audit.

11. RESTRICTED TRANSFERS

- 11.1. The Parties acknowledge that the UK Educational Institution's transmission of Institution Personal Data to CSM in its use of the Digital Citizenship Offering involves a Restricted Transfer, and therefore to ensure that such transmission of Institution Personal Data to CSM does not contravene applicable requirements of Chapter V of the UK GDPR, a 'transfer mechanism' is required.
- 11.2. In relation to the Restricted Transfer noted above and any associated Processing, the Parties shall comply with their respective obligations set out in the Standard Contractual Clauses in the form attached as Annex 4, which are hereby deemed to be entered by and between the Parties –

with the appendices to those Standard Contractual Clauses deemed to have been populated as follows:

- (a) Appendix 1 shall be populated with the corresponding information set out in Annex 1 (*Data Processing Details*); and
- (b) Appendix 2 shall be populated as follows:

“The technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are those established and maintained under Paragraph 4 of the Data Processing Addendum [(including Annex 3)(Security Measures)]”.

- 11.3. CSM may on notice vary this Data Processing Addendum and replace the Standard Contractual Clauses attached as Annex 4 and entered into pursuant to Paragraph 11.2 with any new form of the Standard Contractual Clauses issued or approved by the UK Government or the ICO under Article 46 of the UK GDPR, which shall be suitably populated having regard to the relevant Restricted Transfer to which such updated Standard Contractual Clauses are to be applied.

12. VARIATION

- 12.1. CSM reserves the right to amend this Data Processing Addendum from time-to-time (including by posting an updated form hereof on the page on which this document is currently posted or any successor page thereto), provided always that in its amended form this Data Processing Addendum contains such contractual terms as may then be required by applicable Data Protection Laws.
- 12.2. In the event that the UK Educational Institution does not wish to continue to use the Services following any such variation it may terminate the agreement formed between the Parties under the Terms of Service in its entirety with immediate effect.

13. ORDER OF PRECEDENCE

- 13.1. This Data Processing Addendum shall be incorporated into and form part of the Terms of Service.
- 13.2. In the event of any conflict or inconsistency between:
 - (a) this Data Processing Addendum and the Terms of Service, this Data Processing Addendum shall prevail; or
 - (b) any Standard Contractual Clauses entered into pursuant to Paragraph 11.2 and this Data Processing Addendum and/or the Terms of Service, those Standard Contractual Clauses shall prevail **provided that**, it is agreed that the following shall apply:
 - (i) in the event of any request under Clause 5(j) of the Standard Contractual Clauses that CSM provide copies of any Subprocessor agreement(s) to the UK Educational Institution, CSM may remove or redact all commercial information or all or part of any clauses, recitals, schedules annexes, appendices etc., unrelated to the Standard Contractual Clauses or their equivalent beforehand;

- (ii) the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be performed in accordance with Paragraph 9.1, and shall be subject to any relevant conditions, limitations or restrictions therein;
- (iii) any authorisations or approvals of current and future Subprocessors given to CSM pursuant to Paragraph 5 will constitute the UK Educational Institution's prior written consent to the subcontracting by CSM of the Processing of Institution Personal Data if and as such consent is required under Clause 5(h) of the Standard Contractual Clauses; and
- (iv) certification of deletion of Institution Personal Data as described in Clause 12(1) of the Standard Contractual Clauses shall be provided only upon the UK Educational Institution's written request.

REMAINDER OF PAGE INTENTIONALLY BLANK

Annex 1 Data Processing Details

This Annex 1 to the Data Processing Addendum includes certain details of the Processing of Institution Personal Data as required:

- by Article 28(3) of the UK GDPR; and
- to populate Appendix 1 to the Standard Contractual Clauses attached as Annex 3.

CSM activities

Amongst other things, CSM is a US-based provider of certain Digital Citizenship educational tools and services (including curricula, lesson plans, quizzes and/or tests) for use by Educators with Students at UK Educational Institutions.

UK Educational Institution activities

The UK Educational Institution is an educational institution in the United Kingdom.

Subject matter and duration of the Processing of Institution Personal Data

The subject matter and duration of the Processing of the Institution Personal Data are set out in the Terms of Service and this Data Processing Addendum.

Nature and purpose of the Processing of Institution Personal Data

CSM Processes Institution Personal Data in order to perform the Services pursuant to the Terms of Service and as further instructed by the UK Educational Institution in accordance with this Data Processing Addendum.

The categories of Data Subject to whom the Institution Personal Data relates

- Students
- Educators (when not acting as users of the Digital Citizenship Offering)
- Other Data Subjects whose Personal Data is Made Available by the UK Educational Institution, Educators and/or Students in the use or operation of the Digital Citizenship Offering (including in the population of answers in any quizzes, tests or similar (“**Quizzes**”)).

The types of Institution Personal Data to be Processed

- **Educators.**

First and last name, email address, classroom ID assigned from Education Platform.

- **Students.**

First and last name, approximate age (inferred from class), unique pseudonymous identifier assigned by the Education Platform (“**Unique ID**”), and information relating to Quizzes (including dates, times and duration of Quizzes, as well as answers, ranking, scores, grades and results).

Please note:

- When an Educator requests a “class roster” or individual “Student” Quiz report, CSM loads the Educator’s requested Unique IDs and matches those Unique IDs with the Education Platform to create and display a class roster Quiz report for the entire class, or individual Student report to produce a listing that includes Student names paired with Quiz scores.
- CSM does not itself store or retain any class or individual Student Quiz report data.

- **General.**

Any other Personal Data (which may include Special Categories of Personal Data) comprised within Institution Inputs (including in the population of answers any in Quizzes).

The obligations and rights of the UK Educational Institution

The obligations and rights of the UK Educational Institution are set out in the Terms of Service and this Data Processing Addendum.

Annex 2 Subprocessors

Subprocessor:	Brief details of Processing activities:	Address of Subprocessor (and location(s) of Processing activities if different):
Learning Pool (Learning Locker)	Stores unique pseudonymous identifier and quiz results.	77 Sleeper St., One Separt Square, Boston, MA 02210 (with additional offices in UK and Ireland) UK, US, EU

Annex 3 Security Measures

As from the Addendum Effective Date, CSM will implement and maintain the security measures set out in this Annex 3 (“**Security Measures**”).

1. Organizational management and dedicated staff time responsible for the development, implementation and maintenance of CSM's information security program.
2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to CSM's organization, monitoring and maintaining compliance with CSM's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.
3. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available and industry standard encryption technologies for Personal Data that is:
 - (a) transmitted over public networks (i.e. the Internet) or when transmitted wirelessly; or
 - (b) at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).
4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access when employment terminates or changes in job functions occur).
5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that CSM passwords that are assigned to its employees must:
 - (a) be at least eight (8) characters in length;
 - (b) not be stored in readable format on CSM's computer systems;
 - (c) have defined complexity; and
 - (d) have a history threshold to prevent reuse of recent passwords.
6. Physical and environmental security of data centre, server room facilities and other areas containing Personal Data designed to:
 - (a) protect information assets from unauthorized physical access,
 - (b) manage, monitor and log movement of persons into and out of CSM facilities, and
 - (c) guard against environmental hazards such as heat, fire and water damage.
7. Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to CSM's technology and information assets.
8. Incident / problem management procedures designed to allow CSM to investigate, respond to, mitigate and notify of events related to CSM's technology and information assets.

9. Network security controls that provide for the use of enterprise firewalls, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
10. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
11. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

CSM may update or modify such Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

COMMON SENSE MEDIA UK DIGITAL CITIZENSHIP DATA PROCESSING ADDENDUM

Annex 3 Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

UK Educational Institution, as defined in the pre-amble to the Data Processing Addendum to which these Standard Contractual Clauses are attached (the **data exporter**)

Common Sense Media, Inc., whose ordinary business address is at 699 8th Street, Suite C150, San Francisco, California 94103, USA (the **data importer**)

each a “**party**”; together “**the parties**”,

HAVE AGREED on the following Contractual Clauses (the **Clauses**) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) “*personal data*”, “*special categories of data*”, “*process/processing*”, “*controller*”, “*processor*”, “*data subject*” and “*supervisory authority*” shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) “*the data exporter*” means the controller who transfers the personal data;
- (c) “*the data importer*” means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) “*the subprocessor*” means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) “*the applicable data protection law*” means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the United Kingdom;
- (f) “*technical and organisational security measures*” means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

COMMON SENSE MEDIA UK DIGITAL CITIZENSHIP DATA PROCESSING ADDENDUM

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the ICO and does not violate the relevant provisions of the United Kingdom);
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;

COMMON SENSE MEDIA UK DIGITAL CITIZENSHIP DATA PROCESSING ADDENDUM

- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

COMMON SENSE MEDIA UK DIGITAL CITIZENSHIP DATA PROCESSING ADDENDUM

- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the United Kingdom.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

COMMON SENSE MEDIA UK DIGITAL CITIZENSHIP DATA PROCESSING ADDENDUM

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the laws of the United Kingdom.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the laws of the United Kingdom.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

COMMON SENSE MEDIA UK DIGITAL CITIZENSHIP DATA PROCESSING ADDENDUM

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**COMMON SENSE MEDIA
UK DIGITAL CITIZENSHIP
DATA PROCESSING ADDENDUM**

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix is deemed to have been populated in accordance Paragraph 11.2(a) of the Data Processing Addendum to which these Standard Contractual Clauses are attached.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix is deemed to have been populated in accordance with Paragraph 11.2(b) of the Data Processing Addendum to which these Standard Contractual Clauses are attached.