ZAPWORKS DATA PROCESSING ADDENDUM

Last updated: **14 December 2020**

Updated to incorporate EU Standard Contractual Clauses

This Data Processing Addendum (**"DPA"**) supplements and forms part of the ZapWorks User Agreement for Business and Education users. Capitalised terms used, but not defined, in this DPA are defined in Section 2 of the ZapWorks Terms of Use.

PART 1: INTRODUCTION

Purpose

This DPA sets out the terms that apply when Personal Data is processed by Zappar Limited (**"Zappar"**) on behalf of an Account Holder as part of the Services, where the Account Holder is acting as a Controller for the purposes of UK or EU Data Protection law or regulation, including the European General Data Protection Regulation (**"GDPR"**) and the GDPR as applied by Chapter 3 of Part 2 of the UK Data Protection Act 2018 (collectively, the **"Data Protection Laws"**). It applies solely to the extent required by the Data Protection Laws and is effective as of 25 May 2018.

Effect of DPA

If a provision of this DPA conflicts with a provision of the User Agreement, then this DPA will control. The User Agreement will remain in full force and effect and will be unchanged except as modified by this DPA. This DPA will terminate automatically upon the expiry or termination of the User Agreement.

Acceptance

Provided that a User Agreement is in force between the Account Holder and Zappar, this DPA shall take effect automatically as between the parties. The parties may also, at the request of the Account Holder, enter into a hard copy version of this DPA which is physically signed by or on behalf of both parties. The parties may also by agreement enter into an individually negotiated data processing agreement provided such agreement satisfies the minimum requirements laid down in the Data Protection Laws.

Defined terms and interpretation

For the purposes of this DPA:

The expressions **"Controller"**, **"Data Subject"**, **"Processor", "Personal Data Breach"** and **"processing"** have the same meaning as in Article 4 of the GDPR;

"**EEA"** means the European Economic Area;

"Personal Data" means any User Content of the Account Holder that is or contains information that relates to an identified or identifiable natural person, to the extent that such information is protected as "personal data" under the Data Protection Laws. This does not include any personal data in respect of which Zappar is the sole Controller under the Data Protection Laws;

"Standard Contractual Clauses" means Annex 3, attached to and forming part of this DPA pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC; and

"UK Act" means the Data Protection Act 2018 of the United Kingdom.

In the case of the processing of Personal Data to which the GDPR does not apply references in this DPA to "Union law", "Member State law", "the law of a Member State" and "Union or Member State law" have effect as references to the domestic law of the United Kingdom.

PART 2: DETAILS OF PROCESSING

Details of Zappar's role as a Processor of Personal Data are as follows:

Subject Matter of the Personal Data processing: The provision of the Services by Zappar to the Account Holder and their Authorised Users.

Duration of the Personal Data processing: The term of the User Agreement and any period after the term prior to Zappar's deletion of all Personal Data included within the User Content.

Nature and purpose of the Personal Data processing: To enable the Account Holder and their Authorised Users to receive and Zappar to provide the Services, including publication, hosting and serving of User Content across Zappar's technology platform.

Categories of Personal Data: In general, this may consist of identifying information and organisation data of the Account Holder's clients, customers and end users and Personal Data of Data Subjects contained in User Content such as images, videos, voices; together with such other categories as are agreed by the parties and recorded in writing. It is acknowledged that Zappar does not allow the Services to be used for the purposes of processing any of the "special categories" of Personal Data specified in Article 9(1) of the GDPR.

Categories of Data Subjects: To the extent User Content contains Personal Data, it may concern the Account Holder's end users, customers, employees, business contacts, members of the public and other individuals who have consented to their Personal Data being included within the Account Holder's User Content.

PART 3: DATA PROCESSING TERMS

1. The roles of the parties. To the extent that Zappar processes Personal Data in the course of providing the Services, it will do so only as a Processor acting on behalf of the Account Holder (who may act either as Controller or Processor with respect to Personal Data) and in accordance with the requirements of this DPA.

2. Scope of processing.

    2.1. Zappar undertakes that it will only process the Personal Data on documented instructions from the Account Holder, including with regard to transfers of Personal Data to a third country or an international organisation, unless Zappar is required to do so by European Union or Member State law to which Zappar is subject; in such a case, Zappar shall inform the Account Holder of that legal requirement before processing, unless that law prohibits such information on important grounds of public

interest. For the purposes of this clause, any processing necessary to provide the Services in the manner requested by the Account Holder or their Authorised User(s) shall be deemed to be a documented instruction to Zappar.

2.2. Zappar shall immediately inform the Account Holder if, in Zappar's opinion, an instruction given by or on behalf of the Account Holder would breach the GDPR or other European Union or Member State data protection provisions.

3. Obligations of the Account Holder.

3.1. The Account holder, as the Controller, shall be responsible for ensuring that: (a) it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including the Data Protection Laws; and (b) it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Zappar for processing in accordance with the terms of the User Agreement and this DPA.

3.2. The Account Holder shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which the Account Holder acquired the Personal Data.

4. Confidentiality. Zappar shall ensure that persons authorised by Zappar to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Security of Data Processing. Zappar shall have in place and maintain throughout the term of this DPA appropriate technical and organisational measures to protect the Personal Data in accordance with the requirements of Article 32 of the GDPR. These measures are described in Annex 1 attached to and forming part of this DPA.

6. Security Breach Notification.

6.1. Zappar shall notify the Account Holder without undue delay after becoming aware of a Personal Data Breach affecting the Personal Data which is the subject of this DPA. Zappar's obligation to report or respond to a Personal Data Breach under this Clause 6 is not and will not be construed as an acknowledgement by Zappar of any fault or liability of Zappar with respect to the Personal Data Breach.

6.2. Notification(s) of Personal Data Breaches, if any, will be delivered to one or more of the Account Holder's administrators by any reasonable means Zappar elects, including via email. It is the Account Holder's sole responsibility to ensure that accurate contact information is maintained for its administrators on the Account Holder's ZapWorks account.

7. Rights of Data Subjects. Zappar shall taking into account the nature of the processing, provide the Account Holder with reasonable assistance by appropriate technical and organisational measures, insofar as this is possible and at the Account Holder's cost, with fulfilling the Account Holder's obligations to respond to requests by Data Subjects to exercise their rights laid down in Chapter III of the GDPR. If a request is made directly to Zappar, Zappar shall promptly inform the Account Holder

8. Other assistance. Zappar shall also provide the Account Holder with reasonable assistance, at the Account Holder's cost, in ensuring compliance with the Account Holder's obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to Zappar.

9. Deletion/ Return of Personal Data. Upon the expiry or termination of the User Agreement, Zappar shall, at the choice of the Account Holder, delete or return to the Account Holder all relevant Personal Data and delete all existing copies unless Union or Member State law requires storage of the Personal Data.

10. Audit rights. Zappar will make available to the Account Holder all information reasonably necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR. Whilst it is the parties' intention ordinarily to rely on the provision of the documentation to verify Zappar's compliance with this DPA, Zappar shall permit the Account Holder (or their appointed third party auditor who must not be a competitor of Zappar) to carry out an audit of Zappar's processing of Personal Data under the User Agreement following a Personal Data Breach suffered by Zappar, or upon the instruction of a data protection authority. The Account Holder must give Zappar reasonable prior notice of such intention to audit, conduct its audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to Zappar's operations. Any such audit shall be subject to Zappar's security and confidentiality terms and guidelines. The Account Holder will reimburse Zappar for any such on-site audit at Zappar's then-current rates, which shall be made available to the Account Holder upon request. The charges for the audit shall be reasonable taking into account the resources expended (or to be expended) by Zappar and where possible shall be agreed by the parties prior to commencement of the audit. If Zappar declines to follow any instruction requested by the Account Holder regarding audits, the Account Holder is entitled to terminate this DPA and the User Agreement. If the Standard Contractual Clauses apply, nothing in this Clause 10 varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

11. Use of sub-processors. The Account Holder agrees that Zappar may engage third party sub-processors (collectively, **"Sub-Processors"**) to process the Personal Data on the Account Holder's behalf, including the sub-processors listed in Annex 2. Zappar shall impose on each Sub-Processor obligations that protect the Personal Data to the same or substantially similar standard provided for by this DPA and shall remain liable for any breach of the DPA caused by a Sub-Processor. Zappar, may by giving reasonable notice, add or make changes to the Sub-Processors. If the Account Holder objects on reasonable grounds to any proposed change (e.g. if making Personal Data available to the Sub-Processor may violate applicable Data Protection Laws or weaken the protections for such Personal Data) it must notify Zappar within 14 calendar days of the date of Zappar's notification. Such notice shall contain the reasonable grounds for the objection. Following receipt of the Account Holder's notice, the parties will work together in good faith to find an alternative solution. If the parties are unable to find an alternative solution acceptable to both of them within a reasonable period of time, which shall not exceed 30 calendar days, and Zappar is unable to continue to provide the Services to the Account Holder without use of the objected-to Sub-Processor, either party may at any time thereafter terminate the User Agreement by written notice to the other, without imposing a penalty for such termination on the Account Holder.

12. Transfers of Personal Data (EU or EEA Account Holder).

12.1. The provisions of this Clause 12 apply as of the 1 January 2021 and where the Account Holder is established in the European Union or European Economic Area (EEA).

12.2. Personal Data will be stored in an Amazon Web Services (AWS) data centre in one of AWS's EU Regions – currently the EU (Dublin Region). Except as agreed otherwise in writing with the Account Holder, Zappar will not transfer Personal Data from this location except as necessary to provide the Services initiated by the Account Holder, their Authorised Users or end users, or as necessary to comply with European Union law or binding order of a governmental body of an EU Member State. The Account Holder acknowledges that although User Content is homed in the European Union, User Content may be distributed worldwide to improve content delivery performance and end user experience. Once User Content has been accessed for the first time, it will then be served from the AWS hub closest to the end user. If the Standard Contractual Clauses apply, nothing in this clause varies or modifies the Standard Contractual Clauses.

12.3. The Standard Contractual Clauses will apply to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR). The Standard Contractual Clauses will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if Zappar has adopted Binding Corporate Rules for Processors or an alternative recognised compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA.

13. Limitation of Liability. Zappar's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to Section 22 (Disclaimers) and Section 23 (Exclusion and Limitation of Liability) of the ZapWorks Terms of Use, and any reference in such sections to the liability of Zappar means the aggregate liability of Zappar under the User Agreement and this DPA.

14. Amendment. Zappar may update and change any part or all of this DPA at any time by posting a new version on zap.works provided that the updated DPA continues to meet the minimum requirements laid down in the Data Protection Laws. When Zappar makes changes the "Last Updated" date will be updated to reflect the date of the most recent version.

15. Governing Law.

15.1. Subject to Clause 15.2 and Clause 15.3, this DPA shall be governed by and construed in all respects in accordance with the laws of England.

15.2. If the Account Holder is established in the European Union or EEA, or either party is subject to the GDPR, the governing law of the DPA shall be the law of the Republic of Ireland.

15.3. If the Contractual Clauses apply by virtue of Clause 12.3, the governing law of the DPA shall be the law of the Member State in which the data exporter is established.

Annex 1

Security Measures

Zappar has put in place the following technical and organisational measures to protect the Personal Data:

1. Zappar has prepared and published documented information security guidelines for staff accessing and dealing with "personal data".

2. Zappar permits staff members to have access to or deal with the Personal Data only as reasonably necessary to provide the ZapWorks service to the Account Holder and their Authorised Users. Zappar employees have contracts which require them to maintain the confidentiality of the information they have access to.

3. Audit logs are maintained of staff access to ZapWorks databases. Staff access is promptly removed when an employee leaves the company.

4. ZapWorks and Zappar's content delivery platform are hosted by Amazon Web Services (AWS). AWS deploy a number of physical security measures to protect their data centres. For more information please see: https://aws.amazon.com/security/

5. Where possible Zappar uses managed services and server images, maintained by AWS. This means Zappar benefits from AWS's ongoing efforts to protect and secure these systems.

6. Remote server access is disabled, where possible. Where remote server access is necessary Zappar: (a) uses industry-standard public key and two-factor authentication practices; and (b) limits access to key individuals.

7. ZapWorks Accounts are protected by access authentication controls. Logs are maintained of all login attempts.

8. Zappar regularly reviews its systems for upstream patching and OS updates.

9. Zappar uses firewalls and virtual private cloud technology to isolate subsystems from each other and the Internet.

10. Zappar regularly scans ZapWorks for vulnerabilities, including OWASP Top 10.

11. Zappar continuously monitor its systems using AWS GuardDuty.

12. Measures are taken to safeguard the continuity of the ZapWorks service by creating backup copies of key databases, but Users should maintain on a regular basis their own backups of files uploaded to ZapWorks.

13. Zappar will conduct periodic reviews of the security of its systems to identify whether additional or different security measures may be required.

Annex 2

Sub-Processors

Company name and address	**Type of processing activities performed**	**Data storage location**
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855, Luxembourg	Content hosting and serving, including transmission of content through the cloud.	Primary storage location is in Ireland, but content may be cached locally to improve content delivery performance

Annex 3

Standard Contractual Clauses (processors)

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

The individual or entity identified as "Account Holder" in the DPA
(the "**data exporter**")

and

Zappar Limited
Barley Mow Centre, 10 Barley Mow Passage, London W4 4PH, United Kingdom
(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 Member State in which the data exporter is established;

(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.

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 relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(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;

(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;

(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 of 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 Member State in which the data exporter is established.

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.

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 law of the Member State in which the data exporter is established.

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.

2. 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.

3. 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.

4. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

5. 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
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.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is the individual or entity identified as "Account Holder" in the DPA

Data importer

The data importer is Zappar Limited, a provider of augmented reality technology, including ZapWorks an AR toolkit which can be used by individuals and businesses to create and publish their own augmented reality content on Zappar's technology platform.

Data subjects

Data subjects are defined in Part 2 of the DPA.

Categories of data

The personal data are defined in Part 2 of the DPA.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

The processing operations are defined in Part 2 of the DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organisational security measures implemented by the data importer are as described in the DPA.