

<https://eRevision.uk> Data Processing Agreement (DPA)

Preamble

The ICO states that DPAs must contain the following elements at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/contracts/>

These are in blue and are cross-referenced within the contract:

- ❶ the subject matter and duration of the processing;
- ❷ the nature and purpose of the processing;
- ❸ the type of personal data and categories of data subject;
- ❹ the Data Controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- ❺ processing only on the Data Controller's documented instructions;
- ❻ the duty of confidence;
- ❼ appropriate security measures;
- ❽ using sub processors;
- ❾ data subjects' rights;
- ❿ assisting the Data Controller;
- ⓫ end-of-contract provisions; and audits and inspections.

For UK schools & organisations:

- ⓬ the UK Addendum for International Transfer also applies;

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between the organisation using eRevision listed at the end of this agreement (the "**Company**") and ZigZag Education (the "**Data Processor**") (together as the "**Parties**")

WHEREAS

(A) The Customer (the "Company") acts as a Data Controller. When the Company (school, college, teacher or other entity) orders an eRevision package from ZigZag Education for their students, ZigZag Education becomes a Data Processor for which the Company is the Data Controller. This contract shall become effective on the date of both Parties' signatures. Both Parties shall be entitled to require the contract renegotiated if changes to the law or inexpediency of the contract should give rise to such renegotiation. The contract shall apply for the duration of the provision of personal data processing services. ❺

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor. The purpose of the processing is to support students' learning, practice and revision, teachers' management of the students' activities, and associated administrative activities. These activities take place on the <https://eRevision.uk> website. ❷

The subject matter of the processing is students' and teachers' Personal Data. The duration of the processing is determined by the Company and is ongoing until the Company gives notice that it wishes to terminate this agreement. ❶

Personal Data that is submitted to eRevision by the Company can include but is not limited to: names, email addresses, IP addresses, passwords, subjects, package subscriptions, target grades, answers and activity scores. ❸

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

IT IS AGREED AS FOLLOWS:

1. Definitions

"Data Protection Laws"	means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
"EU Data Protection Laws"	means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
"GDPR"	EU General Data Protection Regulation 2016/679
"UK"	The United Kingdom of Great Britain and Northern Ireland.
"UK GDPR"	As defined in section 3 of the Data Protection Act 2018.
"Data Transfer"	a transfer of Personal Data from the Company to a Data Processor; or an onward transfer of Personal Data from a Data Processor to a Sub Processor, or between two establishments of a Data Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);
"Services"	means the Education services the Company provides
"Sub Processor"	means any person appointed by or on behalf of Data Processor to process Personal Data on behalf of the Company in connection with the Agreement
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed

The terms "Commission", "Data Controller", "Data Processor", "Data Subject", "Member State", "Personal Data", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. The Data Controller's Obligations and Rights

1. The Data Controller is responsible for ensuring that the processing of Personal Data takes place in compliance with the GDPR.
2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of Personal Data.
3. The Data Controller shall be responsible for ensuring that the processing of Personal Data, which the Data Processor is instructed to perform, has a legal basis. ④

3. Data Processor Personnel

The Data Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of the Data Processor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with applicable laws in the context of that individual's duties to the Data Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality. ⑥

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 of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall, in relation to the Personal Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. These include:
 - a) Security measures to protect the web servers holding the data
 - b) Security planning and measures in the programming of the eRevision website
 - c) Security of backup copies for recovery in the event of corruption or failure
 - d) User passwords are stored in encrypted format in an encrypted database
 - e) Internal training, procedures and periodic review of security measures

- 4.2 In assessing the appropriate level of security, the Data Processor shall take into account the risks that are presented by Processing, in particular those from a Personal Data Breach. 7

5. Sub Processing

The Data Processor shall not appoint (or disclose any Personal Data to) any Sub Processor unless required or authorized by the Company. The Data Processor has the Data Controller's general authorisation for the engagement of Sub Processors. The Data Processor shall inform in writing the Data Controller of any intended changes concerning the addition or replacement of Sub Processors at least 1 calendar month in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned Sub Processor(s). The Data Processor must put in place a contract imposing the same GDPR Article 28 data protection obligations on its Sub Processors. The list of current Sub Processors is as follows: 8

Sub Processor	Service	Notes
Digital Ocean	Web hosting on UK located server	Digital Ocean has ISO/IEC 27001:2013 Certification. Standard EU clauses are included in their DPA as well as the UK IDTA Addendum: https://www.digitalocean.com/legal/data-processing-agreement
Amazon SES	Email routing through a UK located server	AWS (Amazon Web Services) has ISO/IEC 27001:2013, 27017:2015, and 27018:2019 Certification. Standard EU clauses are included in their DPA as well as the UK IDTA Addendum: https://aws.amazon.com/service-terms/

6. Data Subject Rights

- 6.1 Taking into account the nature of the Processing, the Data Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company's obligations, as reasonably understood by the Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws. 9^{1of2}
- 6.2 The Data Processor shall:
- promptly notify the Company if it receives a request from a Data Subject (Data Subject Access Request, SAR) under any Data Protection Law in respect of Personal Data; 9^{2of2}
 - ensure that it does not respond to that request except on the documented instructions of the Company or as required by Applicable Laws to which the Data Processor is subject, in which case the Data Processor shall, to the extent permitted by Applicable Laws, inform the Company of that legal requirement before the Data Processor responds to the request.

7. Personal Data Breach

- 7.1 The Data Processor shall notify the Company without undue delay upon the Data Processor becoming aware of a Personal Data Breach affecting Personal Data, providing the Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- 7.2 Data Processor shall cooperate with the Company and take reasonable commercial steps as directed by the Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach. 10^{1of3}

8. Data Protection Impact Assessment and Prior Consultation

The Data Processor shall provide reasonable assistance to the Company with any data protection impact assessments which the Company reasonably considers to be required by Article 35 or 36 of the GDPR. 10^{2of3}

9. Deletion or Return of Personal Data

If the Data Controller terminates this contract, the Data Processor will delete all personal data from its systems within 1 calendar month, apart from Backup Copies. Backup copies are deleted periodically as part of the backup destruction schedule. The Data Processor will periodically delete activity data more than 5 years old and users that have been inactive for more than 5 years. 10^{3of3}

10. Audit Rights

- 10.1 The Data Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to Processing of the Personal Data by the Data Processor. The Data Processor shall tell the Data Controller immediately if it is asked to do something infringing the GDPR. ¹¹
- 10.2 Unless granted elsewhere in this Agreement, the scope of information and audit rights of the Company under section 10.1 are limited to the extent required by Data Protection Law.

11. Data Transfer

If personal data processed under this Agreement is transferred from the area encompassing the UK and the European Economic Area (UK+EEA) to a country outside the UK+EEA, the Parties shall ensure that the Personal Data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU-approved standard contractual clauses for the transfer of Personal Data.

In addition, where the Data Controller is in the UK, each Party agrees to be bound by the terms and conditions set out in the Addendum below, in exchange for the other Party also agreeing to be bound by this Addendum. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs. ¹²

12. General Terms

All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out below or at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

This Agreement including the Addendum is governed by the laws of England. Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of England and Wales, subject to possible appeal to the High Court in London.

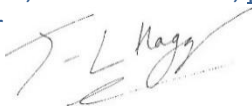
IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

ZigZag Education ("Data Processor")

Unit 3, Greenway Business Centre, Doncaster Road, Bristol BS10 5PY, privacy@ZigZagEducation.co.uk

Name: John-Lloyd Hagger Position: Partner

Date Signed: 23th February 2023



Organisation using eRevision ("Company", "Data Controller"):

Organisation: _____

Correspondence address: _____

Name: _____ Position: _____

Signature: _____ Date signed: _____

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

- Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

"Addendum"	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
"Addendum EU SCCs"	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
"Appropriate Safeguards"	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
"Approved Addendum"	This Addendum based on that issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022.
"Approved EU SCCs"	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
"ICO"	The Information Commissioner.
"Parties"	ZigZag Education and the Organisation using eRevision
"Restricted Transfer"	A transfer which is covered by Chapter V of the UK GDPR.
"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.

- This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
- If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
- If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
- If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
- 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, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

- Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 8 will prevail.
- Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
- Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

10. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
 - a. together they operate for data 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 data transfer, and they provide Appropriate Safeguards for those data transfers;
 - b. Sections 7 to 9 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
11. Unless the Parties have agreed alternative amendments which meet the requirements of Section 10, the provisions of Section 13 will apply.
12. No amendments to the Approved EU SCCs other than to meet the requirements of Section 10 may be made.
13. The following amendments to the Addendum EU SCCs (for the purpose of Section 10) are made:
 - a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
 - b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
 - c. 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.";
 - d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
 - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
 - f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
 - g. References to Regulation (EU) 2018/1725 are removed;
 - h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
 - i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";
 - j. Clause 13(a) and Part C of Annex I are not used;
 - k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
 - l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;"
 - m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";
 - n. Clause 18 is replaced with:

"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."; and
 - o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.