Oct 2023 - V2.0

Qoria Legal Agreements

Data Processing Addendum

qoria.com

Qoria

Introduction

This Data Processing Addendum (“DPA”) forms part of the Terms of Service of Qoria Ltd (“Qoria”, or we, or us). This DPA shall be read in conjunction with (and takes priority over) our Privacy Policy which forms part of our Terms of Service.

Definitions

All terms with capitalised initial letters that are defined in the General Data Protection Regulation 679/2016) (“GDPR”) have the same meaning provided in that regulation.

“Customer” or “you” means the entity that accepts our Terms of Service and DPA directly or through our resellers.

“Customer Data” means all data that Qoria collects and processes under the Customer’s instructions in order to provide the Service. In particular, it means the data listed in the Privacy Policy.

“Applicable Data Protection Legislation” means:

1.) Data Protection Legislation:

- The GDPR: The General Data Protection Regulation 679/2016, a European Union (EU) legal framework that sets out guidelines for the collection and processing of personal data;
- The UK GDPR: With respect to the United Kingdom, the GDPR as retained in UK law by virtue of section 3 of the UK European Union Act 2019 (“UK GDPR”) and the Data Protection Act 2018 (together, “UK Data Protection Acts”). In the event that the UK decides to replace the UK GDPR with a data protection law of its own, the UK Data Protection Laws will include such law; and
- Swiss DPA: the Swiss Federal Data Protection Act and its implementing regulations; and

2.) Comparable Regulations being laws in other jurisdictions which govern controllership and processing of data and limit transborder flows of data.

Applicability & Scope

This DPA applies only to the extent that we process, on your behalf Customer Data to which Applicable Data Protection Legislation applies. Applicable Data Protection Legislation is:

A.) Data Protection Legislation being GDPR: The General Data Protection Regulation, a European Union (EU) legal framework that sets guidelines for the collection and processing of personal information; UK GDPR: In respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2019 ("UK GDPR") and the Data Protection Act 2018 (together, "UK Data Protection Laws"); and Swiss DPA: the Swiss Federal Data Protection Act and its implementing regulations; and

B.) Comparable Regulations being laws in other jurisdictions which govern controllership and processing of data and limit transborder flows of data.

We undertake to comply with Data Protection Legislation in our provision of Products and Services to you.

You undertake to ensure that your instructions comply with Applicable Data Protection Legislation. You acknowledge that we are neither responsible for determining which laws are applicable to you nor whether our Products and Services meet or will meet the requirements of such laws. You undertake to ensure that our processing of Customer Data, when done in accordance with your instructions, will not cause us to violate any applicable law, including Applicable Data Protection Legislation. We undertake to inform you if we become aware, or reasonably believe, that your instructions violate applicable law, including Applicable Data Protection Legislation.

Processing of Customer Data as Data Processor

In the context of the processing of Customer Data, we undertake to:

a) Ensure that staff members authorised to process data have undertaken to respect the confidentiality of Customer Data, or are subject to a confidentiality obligation of a statutory nature;

b) Implement the necessary measures to ensure the security of Customer Data, as indicated in the "Security" section;

c) Use other processors only with the authorization of the Data Controller, as provided for in the "Sub-processors" section;

d) Assist you (as the Data Controller), taking into account the nature of the processing, through appropriate technical and organisational measures, whenever possible to fulfil your obligations to respond to requests aimed at exercising the rights of data subjects;

e) Assist you (as the Data Controller) to ensure compliance with the obligations set out in GDPR Articles 32 to 36, taking into account the nature of the processing and the information available to the processor;

f) Delete all personal data upon termination of the provision of processing services, and shall delete existing copies unless the retention of personal data is required by the Applicable Data Protection Legislation;

g) Adhere to codes of conduct or other certification mechanisms, if they exist and are applicable;

h) Make available to relevant persons in your organisation all information necessary to demonstrate compliance with the obligations set forth in GDPR Article 28,, as well as to allow and contribute to the performance of audits, including inspections, by the person in charge or by another auditor authorised by said person in charge.;

i) If you are located in the European Union, Comply with the European Union model contractual clauses for international data transfers included in Annex 1.; and

j) If you are located in the UK, comply with the European Union model contractual clauses for international data transfers included in Annex 1, and the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses in Annex 2. .

You undertake to ensure that: a) all notices have been given, and all such authorizations have been obtained, as required under Applicable Data Protection Legislation, for us (and any sub-processors) to process Customer Data as contemplated by our Customer Agreement and this DPA;.

Sub-Processors

A “sub-processor” means any third-party data processor engaged by us to assist us to fulfill our obligations under your Customer Agreement and which processes Customer Data. Sub-processors may include third parties or our affiliates. You agree that (a) we may engage sub-processors (as listed on our website, https://qoria.com/privacy/sub-processors) which may change from time to time; and (b) such sub-processors respectively may engage third party processors to process Customer Data on our behalf.

You provide a general authorization for us to engage onward sub-processors subject to these conditions: a) we will restrict the onward sub-processor’s access to Customer Data only to what is strictly necessary to provide the Services, and we will prohibit the sub-processor from processing the Customer Data for any other purpose; b) we agree to impose contractual data protection obligations, including appropriate technical and organizational measures to protect Customer Data, on any sub-processor we appoint that require suchsub-processor to protect Customer Data to the standard required by Applicable Data Protection Legislation; and c) we will remain liable and accountable for any breach of this DPA that is caused by an act or omission of our sub-processors.

We may, by giving reasonable notice to you, add or remove sub-processors. Where we do so we undertake to update the schedule of processors (as listed on our website https://qoria.com/privacy/sub-processors) at least 10 days prior to any change. If you object on reasonable grounds (in our sole opinion, acting reasonably) to such a change then we agree to work with you on a good faith basis to find an alternative solution. In the event that the parties are unable to find such a solution, you may terminate the Agreement at no additional cost.

Audits & Assistance

We shall, to the extent required by Applicable Data Protection Legislation, provide you with reasonable assistance (at your cost) with data protection impact assessments or prior consultations with data protection authorities that you are required to carry out under such legislation.

We acknowledge that as a data processor on your behalf, you must be able to assess our compliance with our obligations under Applicable Data Protection Legislation and this DPA. We agree to make available to you all information reasonably necessary to demonstrate compliance with this DPA and Applicable Data Protection Legislation.

We agree to permit you (or your appointed third party auditors) to carry out an audit at your cost (including without limitation our costs) following a security breach suffered by us, or upon the instruction of a data protection authority acting pursuant to Applicable Data Protection Legislation. You agree to provide us with reasonable prior notice of such a requirement, conduct an audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to our operations. Any such audit shall be subject to our security and confidentiality terms and guidelines and may only be performed a maximum of once annually. If we decline to follow any reasonable instruction from you regarding such an audit, then you are entitled to terminate your Customer Agreement.

In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Legislation or (b) any Third Party Request relating to the processing of Account Data or Customer Data conducted by the other party, such party will promptly inform the other party in writing. The parties agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Legislation.

Data Transfers

You acknowledge that we and our sub-processors may transfer and process your Customer Data outside of your jurisdiction, including in the United States of America. We undertake to ensure that such transfers are made in compliance with

Applicable Data Protection Legislation and this DPA. Applicable Data Protection Legislation may impose restrictions on or require Standard Contractual Clauses ("SCCs") with respect to transborder data transfers. Where SCCs apply (as amended or superseded) these are incorporated into this DPA and your Customer Agreement. The parties acknowledge that to the extent the SCC's conflict with any provision of your Customer Agreement (including this DPA) then the SCCs prevail to the extent of the conflict.

Security

We have in place and maintain appropriate measures designed to protect your Customer Data. We undertake to ensure these measures comply with applicable law. We undertake to ensure our employees and contractors are appropriately trained in security and privacy and are subject to duty of confidentiality.

Should we become aware of a security breach we undertake to comply with local laws and notify you without undue delay and provide you such information as you may reasonably require, including to enable you to fulfil your reporting obligations under Applicable Data Protection Legislation. You acknowledge that notification of or response to a security breach is not an acknowledgement by us of any fault or liability.

You are solely responsible for use of our Products, and you are responsible for (a) ensuring your End-Users are adequately informed about our Product's processing of their data.

End of Contract

Upon termination or expiry of your Customer Agreement, we will delete and/or deliver to you your Customer Data in accordance with our Privacy Policy and Terms of Service.

Representative in the European Union
In order to comply with the provisions of the GDPR, we have appointed a data protection representative in accordance with GDPR Article 27. Our EU representative acts as a point of contact for data protection authorities and data subjects on matters relating to personal data protection. You may contact our EU representative via the contact details provided below:

EU Representative: Qustodio Technologies, S.L.U.
Address: Roger de Flor 193, bajos, 08013, Barcelona, Spain
Contact email: dpo@qustodio.com

Representative in the United Kingdom
In order to comply with the provisions of the GDPR, we have appointed a data protection representative in accordance with Article 27. Our UK representative acts as a point of contact for data protection authorities and data subjects on matters relating to personal data protection. You may contact our UK representative via the contact details provided below:

UK Representative: Smoothwall Limited.
Address: Second Floor, 2 Whitehall Quay,
Leeds LS1 4HR, United Kingdom
Contact email: privacy@qoria.com

Annex 1 – EU Standard Contractual Clauses for international transfers of data

Section I

Clause 1 - Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) () for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex 3 Table 1 (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex 3 Table 1 (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex 3 Table 3

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 - Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 - Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 - Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 - Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex 3 Table 3.

Section II – Obligations of the Parties

Clause 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 3 Table 3, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex 4 and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex 3 Table 3. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or

returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex 4. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex 3 Table 3.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter

all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 - Use of sub-processors

The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s).
The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(a) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(b) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(c) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(d) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 - Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 - Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 - Supervision

The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

Section III – Local Laws and Obligations in Case of Access by Public Authorities

Clause 14 - Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that

there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Section IV – Final Provisions

Clause 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
    (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
    (ii) the data importer is in substantial or persistent breach of these Clauses; or
    (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 - Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Spain.

Clause 18 - Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of Spain.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ntering into this Addendum
Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
Although Annex 1 Table 1 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.

Annex 2 – UK GDPR International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1 Table 1 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.

Interpretation of this Addendum

3. 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 EU SCCs included in Annex 1.

Addendum EU SCCs
The version(s) of the Approved EU SCCs included in Annex 1..

Appendix Information
As set out in Annex 3 Table 2.

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
The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

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.

Restricted Transfer
A transfer which is covered by Chapter V of the UK GDPR.

UK
The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws
All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR
As defined in section 3 of the Data Protection Act 2018.

4. 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.

5. If the provisions within the Addendum EU SCC's 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.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. 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.

8. 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

9. Although Clause 5 of the Addendum EU SCC's sets out that the Addendum EU SCC's prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between this Addendum and the Addendum EU SCC's, this Addendum overrides the Addendum EU SCC's, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCC's provides greater protection for data subjects, in which case those terms will override this Addendum.

11. 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

12. This Addendum incorporates the Addendum EU SCC's 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 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCC's; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Addendum EU SCC's other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCC's (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCC's;

    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 3 Table 3 where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.8(i) is replaced with: "the onward transfer is to a country benefiting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    e. 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;

    f. References to Regulation (EU) 2018/1725 are removed;

    g. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

h. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

i. 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;";

j. Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";

k. 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

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Annex 3, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:
    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws; The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Annex 3 Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or
    b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Annex 3 – Data Tables

Table 1: Parties

Start date	As described in the Customer Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	As described in the Customer Agreement	Qoria Ltd
Key Contact	As described in the Customer Agreement	privacy@qoria.com
Signature (if required for the purposes of Section 2)	Each parties signature to the Customer Agreement is considered signature to the addendum	

Table 2: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

List of Parties:	as set out above
Description of Transfer:	as described below
Technical and organisational measures to ensure the security of the data:	as set out in Annex 4
List of Sub processors:	as described at https://qoria.com/privacy/sub-processor

Table 3: Description of Transfer

Categories of data subjects whose personal data is transferred	as described in the Customer Agreement
Categories of personal data transferred	as described in the Customer Agreement
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	as set out in Annex 4
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Continuous basis
Nature of the processing	As defined within the Qoria privacy policy available at www.qoria.com/privacy
Purpose(s) of the data transfer and further processing	As defined within the Qoria privacy policy available at www.qoria.com/privacy
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	As defined within the Qoria privacy policy available at www.qoria.com/privacy
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	As defined within the Qoria privacy policy and the list of sub processors available at www.qoria.com/privacy

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer Exporter neither Party

Annex 4 - Technical and organisational measures to ensure the security of the data

Qoria (including Linewize, Smoothwall, Qustodio and Educator Impact) take privacy and security of customer data very seriously. We choose to exclusively use Tier 1 data centres provided by Microsoft, Amazon and Google. These data centres facilitate us deploying security and resilience of the highest order.
Your data is encrypted in transit and at rest when stored in the data centre using industry standard secure encryption technologies.
Internally Qoria have implemented the NIST Cybersecurity Framework and hold any company we deal with to the same high standards.

Safeguards and practices in place to manage personal data

Technical
- Data encryption (transit and rest)
- Endpoint detection and response (EDR)
- Data backups
- Identity and access management

Operational
- Security operations centre (SOC)
- Vulnerability management
- Incident management

Administrative
- Secure-by-design process
- Employee background checks
- Internal & external privacy policy
- Employee security training
- Vendor risk management
- Security policies (ie. vulnerability management, data classification, third party risk management, user & device security policies, DPIA procedure)
- Account management, least privilege and limiting access to customer data;
- We have a user account security policy which requires the use of security controls such as MFA, password managers and password complexity requirements.

- We have a privileged account policy which requires that administrators and cloud admins create user and service accounts that comply with security standards including least privilege.
We have a data classification policy which controls how data is handled, reproduced and disposed of.

Qoria

Contact

e: enquiries@qoria.com

Global headquarters
Qoria Limited
Level 3, 45 St Georges Terrace,
Perth WA 6000, Australia.

qoria.com