

Data Processing Agreement

WHEREAS, Client ("**Controller**") and IQVIA ("**Processor**") have entered into a written (including in electronic form) contract between Client and IQVIA ("**Agreement**") pursuant to which Processor performs certain services ("**Services**") to, or on behalf of Controller.

WHEREAS, during the course of providing Services, Processor may obtain, access or otherwise process Personal Data.

NOW THEREFORE, the parties agree that the below provisions apply to such processing activities performed by Processor in connection with the Services.

DEFINITIONS

"Applicable Law" means directly applicable legislation, laws, regulations in each case, as these may be repealed, re-enacted, amended, overruled or replaced from time to time in those respective jurisdictions where the Services are rendered and/or where Processor receives, collects, uses, discloses or otherwise processes Personal Data pursuant to the Agreement.

"Data Protection Legislation" means the EU General Data Protection Regulation 2016/679 and all other applicable laws relating to processing of Personal Data and privacy that may exist in any relevant jurisdiction with regard to the processing of Personal Data under the Agreement.

"Controller" means Client. Notwithstanding the foregoing, in the event that the Agreement permits Client's affiliates to enter into Statements of Work with Processor or Processor's affiliates, "Controller" shall mean Client's affiliate that is a party to the relevant Statement of Work.

"EU Personal Data" means the processing of Personal Data to which Data Protection Legislation of the European Union, or of a Member State of the European Union or European Economic Area, was applicable prior to its processing by the Processor."

General Data Protection Regulation" or "**GDPR**" means Regulation (EU) 2016/679;

"FADP" means the Swiss Federal Act on Data Protection.

"Personal Data" shall have the meaning given by the Data Protection Legislation and be provided by Controller to Processor and/or its Subprocessors or collected or processed by Processor and/or its Subprocessors for and on behalf of Controller in the performance of the Services by Processor under the Agreement.

"Processor" means IQVIA. Notwithstanding the foregoing, in the event that the Agreement permits IQVIA's affiliates to enter into Statements of Work with Controller or Controller's affiliates, "Processor" shall mean IQVIA's affiliate that is a party to the relevant Statement of Work.

"Protected Area" means:

- i. in the case of EU Personal Data, the members states of the European Union and the European Economic Area and any country, territory, sector or international organisation in respect of which an adequacy decision under Art.45 GDPR is in force;

- ii. in the case of UK Personal Data, the United Kingdom and any country, territory, sector or international organisation in respect of which an adequacy decision under United Kingdom adequacy regulations is in force; and
- iii. in the case of Swiss personal data, any country, territory, sector or international organisation which is recognised as adequate under the laws of Switzerland;

“Security Incident” shall have the meaning of a “personal data breach” given by the Data Protection Legislation and be an actual incident that compromises the privacy, security, confidentiality, availability and/or integrity of the Personal Data.

“Standard Contractual Clauses/SCCs” mean

- i. the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 including the text from Module Two Clauses (in cases where Processor is established outside the Protected Area and acts as data importer) and not including any clauses marked as optional, with the exception of clause 9, option 2, or Module Four Clauses (in cases where Processor is established inside the Protected Area and acts as data exporter), and no other module, as set out in full at the IQVIA Customer Support Hub at <https://www.customerservice.iqvia.com> and the IQVIA Customer Portal at <https://www.customerportal.iqvia.com> (“EU Standard Contractual Clauses”)
- ii. provided that, in so far as the FADP was applicable prior to transfer to Processor, any references in the clauses to the GDPR shall refer to the FADP, the term ‘member state’ must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the SCCs and the SCCs shall also protect the data of legal persons until the entry into force of the revised FADP; and
- iii. in respect of UK Personal Data:
 - a. the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 but, as permitted by clause 17 of such addendum, the parties agree to change the format of the information set out in Part 1 of the addendum so that:
 - i. the details of the parties in table 1 shall be as set out in the relevant Statement of Work (a) where Module 2 of the SCCs apply and Controller is established in the UK and Processor is established in a third country as defined by UK GDPR, or (b) where Module 4 of the SCCs apply and Controller is established in a third country as defined by UK GDPR and Processor is established in the UK (with no further requirement for signature);
 - ii. for the purposes of table 2, the addendum shall be appended to the EU Standard Contractual Clauses available at the link above (including the selection of modules and disapplication of optional clauses noted above and the selection of the option and timescales for clause 9 set out at that link);
 - iii. the appendix information listed in table 3 is set out at that link; and

- iv. for the purposes of table 4, either party may end the addendum as set out in clause 19 of said addendum.

“Subprocessor” means any third party that Processor engages in accordance with the Agreement to process Personal Data on behalf of Processor in order to provide the Services;

“UK Personal Data” means the processing of Personal Data to which Data Protection Legislation of the United Kingdom was applicable prior to its processing by the Processor;

and

"data controller", "data processor", "data subject", "personal data breach", "processing", and "appropriate technical and organisational measures" shall be interpreted in accordance with the General Data Protection Regulation.

1. DATA PROTECTION

- 1.1 The parties agree that the Controller is the data controller and the Processor is the data processor for purposes of the provision of the Services.
- 1.2 The subject-matter of the data processing is the performance of the Services. The obligations and rights of the Controller are as set out in this Data Processing Agreement. The Personal Data that will be processed pursuant to the Services shall be as set out in the form attached as Annex I to the SCCs and shall form part of each work order concluded under the Agreement or other relevant services agreement (whether or not the SCCs are applicable). Annex I to the SCCs sets out the nature, duration and purpose of the processing, the types of Personal Data the Processor processes and the categories of data subjects whose Personal Data is processed.
- 1.3 When the Processor processes Personal Data, the Processor shall, notwithstanding anything to the contrary in this Agreement :
 - 1.3.1 process the Personal Data only in accordance with written lawful and reasonable instructions of the Controller (which may be specific instructions or instructions of a general nature as set out in this Agreement or as otherwise notified in writing by the Controller to the Processor from time to time) and not for the Processor's own purposes. If the Processor is required to process the personal data for any other purpose by European Union or Member State law to which the Processor is subject, the Processor shall inform the Controller of this requirement before the processing, unless otherwise mandated by Applicable Law on important grounds of public interest;
 - 1.3.2 notify Controller promptly if, in Processor's opinion, an instruction for the processing of Personal Data infringes applicable Data Protection Legislation (**“Unlawful Instruction”**). Should Controller insist on the Unlawful Instruction Processor reserves the right to either suspend the processing or terminate the Service to which the Unlawful Instruction relates. This suspension or termination will not be deemed a breach of this Data Processing Agreement;
 - 1.3.3 provide reasonable assistance to Controller where required under Data Protection Legislation to enable it to comply with its obligations, including its transparency obligations towards data subject(s), under Data Protection Legislation and at Controller’s cost and expense, unless otherwise agreed. For the avoidance of doubt,

Controller shall be responsible for providing the relevant notices to Processor where required for data subject(s);

- 1.3.4 at Controller's cost and expense unless otherwise agreed, and by taking into account the nature of the processing and by using appropriate technical and organisational measures, and insofar as this is possible, assist Controller to fulfil its obligations to respond to requests from data subjects exercising their rights in connection with their Personal Data processed by Processor and/or its Subprocessor during the course of the Services;
- 1.3.5 implement and maintain appropriate technical and organisational measures commensurate with the nature of the Personal Data to protect the Personal Data against unauthorised or unlawful processing and against a Security Incident. Such measures shall include the provisions of Annex II to the SCCs, which shall apply whether or not the SCCs are applicable, and publish any updates to such measures at the IQVIA Customer Support Hub at <https://www.customerservice.iqvia.com> and the IQVIA Customer Portal at <https://www.customerportal.iqvia.com>.
- 1.3.6 engage Subprocessors for the purposes of processing Personal Data under this Agreement. Controller hereby acknowledges and accepts that Processor may engage any of its affiliates as Subprocessors during the term of the Agreement. A list of third party Subprocessors authorised as of the date of the Agreement is set out in Appendix A attached hereto. Any intended changes concerning the addition or replacement of third party Subprocessors shall be published at <https://www.customerservice.iqvia.com> and the IQVIA Customer Portal at <https://www.customerportal.iqvia.com> in order to give the Controller the opportunity to object to such change. If Controller has a legitimate reason under Data Protection Legislation to object to the new Subprocessors' processing of Personal Data, Controller may terminate the Agreement (limited to the Services for which the new Subprocessor is intended to be used) on written notice to Processor within 15 business days of such publication. Such termination shall take effect at the time determined by the Controller which shall be no later than 30 days from the date of Processor's publication of such intended change.
- 1.3.7 ensure the reliability and competence of the Subprocessor(s) and Processor shall include in any contract with the Subprocessor(s) provisions which are no less stringent than those contained in this Data Processing Agreement;
- 1.3.8 remain fully liable to Controller for the fulfilment of Processor's obligations under this Data Processing Agreement, where such Subprocessor fails to fulfil its obligations under the applicable subprocessing agreement or any applicable Data Protection Legislation;
- 1.3.9 bind Processor's personnel who have access to the Personal Data by confidential and non-use obligations no less stringent than the obligations set out in this Data Processing Agreement or under a statutory obligation of confidentiality;
- 1.3.10 upon Controller's written request at reasonable intervals, and subject to reasonable confidentiality controls, Processor will make available to Controller a copy, if available, of either (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) Processor's most recent SOC-2 attestation report to verify the adequacy of its security measures relevant to

Personal Data processed by Processor ("Audit Report"). Controller agrees that any audit rights granted by Data Protection Legislation will be satisfied by these Audit Reports. To the extent that Processor's provision of an Audit Report does not provide sufficient information or Controller is required to respond to a regulatory authority audit, Controller agrees to a mutually agreed-upon audit plan with Processor that: (a) allows Controller or its mandated independent third party auditor to conduct the audit; (b) provides at least ninety (90) days advance notice of any audit to Processor unless Data Protection Legislation or a competent data protection authority requires shorter notice; (c) requests access only during business hours; (d) accepts that Controller shall bear the costs of any audit; (e) occurs no more than once annually; (f) restricts its findings to only data relevant to Controller; and (g) obligates Controller, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

- 1.3.11 maintain, and make available to Controller upon reasonable prior notice, all necessary information and documentation relevant to the Personal Data processing activities in connection with Services performed under the Agreement to verify Controller's compliance with the Data Protection Legislation;
 - 1.3.12 agree, subject to the protection of Processor 's confidential and proprietary information in accordance with the Agreement, that Controller may disclose such information, records and documentation, including this Data Processing Agreement, to demonstrate Controller's compliance with the Data Protection Legislation;
 - 1.3.13 at the end of the Services (1) cease processing the Personal Data except as otherwise provided under Applicable Law and/or (2) destroy or return all copies of Personal Data except as otherwise provided under Applicable Law;
- 1.4 If Processor becomes aware of any Security Incident affecting its processing of Personal Data, Processor shall without undue delay notify Controller and:
- 1.4.1 provide Controller with as detailed a description as possible of the Security Incident;
 - 1.4.2 take action immediately, at Processor 's own expense, to investigate the Security Incident and to identify, prevent and mitigate the effects of the Security Incident and carry out any commercially reasonable action to remedy the Security Incident; and
 - 1.4.3 not release or publish any filing, communication, notice, press release, or report concerning the Security Incident unless otherwise agreed with the Controller (except where required to do so by Applicable Law).
- 1.5 Unless specific data localisation terms are agreed in the Agreement or in the applicable work order, Controller acknowledges that the Processor's platform and services are operated, supported and maintained globally. Any transfer of Personal Data outside of a Protected Area shall be made with appropriate safeguards in place and in accordance the Data Protection Legislation. Where data protection legislation of any member state of the EU, EEA, Switzerland or the United Kingdom applies to the processing of the Personal Data prior to its processing by Processor and where Processor (or Controller, in cases where Module 4 of the SCCs apply)

is established outside the Protected Area then the parties agree to the terms of the Standard Contractual Clauses as if they were set out here in full

- 1.6 In the event Processor makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Data Protection Legislation, Processor must as soon as practicable following the determination provide Controller notice thereof, and provide such further information and assistance as may be reasonably requested at Controller's expense.
- 1.7 To the extent that the terms contained in the Agreement conflict or are inconsistent with those contained in this Data Processing Agreement, the terms contained in this Data Processing Agreement shall control to the extent of such conflict or inconsistency.

APPENDIX A

List of Authorised Third Party Subprocessors

IQVIA uses certain platform Subprocessors, as well as infrastructure suppliers and other third-party business partners, to provide services to its customers. The list of third party Subprocessors authorised as of the effective date of the Agreement is available at <https://www.customerservice.iqvia.com> and the IQVIA Customer Portal at <https://www.customerportal.iqvia.com>. Subprocessors providing professional services are set forth in the relevant Statement of Work.