QorusDocs

Global Data Processing Agreement

Last Modified: 05/07/2024

PLEASE READ THIS DATA PROCESSING ADDENDUM ("ADDENDUM") CAREFULLY BEFORE USING THE WEBSITE, SOFTWARE, OR SERVICES OFFERED BY QORUS SOFTWARE INC. ("QORUS" OR "PROCESSOR"). THIS ADDENDUM SHALL APPLY TO THE EXTENT QORUS IS A PROCESSOR OF PERSONAL DATA (DEFINED BELOW) THAT IS SUBJECT TO CERTAIN DATA PROTECTION LAWS (DEFINED BELOW). YOU OR THE ENTITY YOU REPRESENT AGREE THAT YOU HAVE READ AND ACCEPT THE TERMS IN THIS ADDENDUM, WHICH SUPPLEMENT THE QORUS MASTER SAAS AGREEMENT AS AND ANY ORDER FORM ENTERED INTO BY AND BETWEEN YOU AND QORUS (IN EACH CASE, THE "AGREEMENT").

This Addendum supplements the Agreement only when and to the extent that a customer of Qorus' Subscription Service provides Qorus with personal data that is or will be subject to Data Protection Laws (for the purposes of this Addendum, each customer who does so shall be referred to as a "Controller"). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control.

1. Definitions

1.1 "Affiliate" means any corporation, partnership, or other entity now existing or hereafter organized that directly or indirectly controls, is controlled by, or under common control with a Party. For purposes of this definition "control" means the direct possession of a majority of the outstanding voting securities of an entity.

1.2 "Anonymous Data" means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person.

1.3 "Authorized Employee" means an employee of Processor who needs to know or otherwise access Personal Data to enable Processor to perform their obligations under this Addendum or the Agreement.

1.4 "Authorized Sub-Processor" means a third-party who needs to know or otherwise access Personal Data to enable Processor to perform its obligations under this Addendum or the Agreement, and who are authorized by Controller to do so under Section 4.2 of this Addendum.

1.5 "Canadian Data Protection Law" means, as applicable, the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, the *Personal Information Protection Act*, R.S.A. 2003, c. P-6.5, the *Personal Information Protection Act*, R.S.B.C. 2003, c. 63 and *an Act respecting the protection of personal information in the private sector*, CQLR, c. P-39.1, as amended by Law 25, An Act to modernize legislative provisions as regards the protection of personal information.

1.6 "CCPA" means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199), the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 999.300 to 999.337), as amended by the California Privacy Rights Act of 2020 (CPRA) (Effective January 1, 2023), and any related regulations or guidance provided by the California Attorney General. Terms defined in the CCPA, including "business", "business purposes", "consumer", "personal information", "sale", "sell", "selling", and "service provider" carry the same meaning in this Addendum.

1.7 ""Commissioner" means, in the UK, the UK Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

1.8 "Controller" shall mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.9 "Controller Personal Information" shall mean, as further described in Annexes A-1 and A-2 (as applicable), the Personal Data or Personal Information (as applicable) which Qorus is Processing as Processor on behalf of Controller in order to provide the Services.

1.10 "Data Protection Laws" means all data protection and privacy laws applicable to the respective Party in its role in the processing of Personal Data under the Agreement, including where applicable and without limitation the Canadian Data Protection Law, the EU Data Protection Law, the Swiss Data Protection Law, the UK Data Protection Law, and the U.S. Data Protection Law.

1.11 "Data Subject" means an identified or identifiable person to whom Personal Data relates.

1.12 "EU Data Protection Law" means all applicable privacy and data protection laws in the European Union, including, without limitation, (i) the GDPR, and any equivalent or replacement law in any Member State and all and any regulations made under those acts or regulations; (iii) the Privacy and Electronic Communications Directive (*2002/58/EC*) ("ePrivacy Directive") and any replacement law or regulation in the EU, and any applicable national implementing laws, regulations and secondary legislation in any Member State, in relation thereto; (iv) the guidelines, recommendations, best practice opinions, directions, decisions, and codes of conduct issued, adopted or approved by the European Commission, the European Data Protection Board, and/or any supervisory authority or data protection authority from time to time in relation to the Directive, the GDPR, the ePrivacy Directive, and any other applicable privacy and data protection laws; and (v) any judgments of any relevant court of law relating to the processing of personal data, data privacy, and data security.

1.13 "GDPR" means the EU General Data Protection 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.

1.14 "Instruction" means a direction, either in writing, in textual form (e.g., by e-mail), or by using a software or online tool, issued by Controller to Processor and directing Processor to Process Personal Data.

1.16 "Legitimate Business Purposes" means the exhaustive list of specific purposes for which Company is allowed to Process the Customer Personal Information as Controller as specified in Section 2.5.

1.17 "Member State" means a country that is a member of the European Union or the European Economic Area (Iceland, Liechtenstein, Norway).

1.18 "Personal Data" or "Personal Information" means any information relating to Data Subject or a household (as applicable), which information is subject to Data Protection Laws and which Processor Processes on behalf of Controller other than Anonymous Data.

1.19 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

1.20 "Process", "Processed", "Processes", or "Processing" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.21 "Processor" shall mean a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller or another organization, as applicable.

1.22 "Qorus Security Standards" means the security standards attached to the Agreement, of if none are attached to the Agreement, attached to this Addendum as an Exhibit B.

1.23 "Services" shall mean the Subscription Service as set forth in the Agreement.

1.24 "Swiss Data Protection Law" shall mean the Swiss Federal Data Protection Act of 19 June 1992, as amended by the new Swiss Data Protection Act (the "nDPA"), as of September 1st, 2023.

1.25 "Standard Contractual Clauses" (SCC) means the agreement executed, where applicable, by and between Controller and Processor pursuant to the European Commission's decision 2021/914 of June 4, 2021, on standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection (or any updated version thereof).

1.26 "Supervisory Authority" means the relevant privacy regulator in the territories where the parties to this Agreement are established (other than the Commissioner), including without limitation the California Privacy Protection Agency, and any other U.S., Canadian federal, state, provincial or EU national independent public authority responsible for data protection matters and which is established pursuant to Data Protection Laws.

1.27 . "Transfer" shall mean the access by, transfer or delivery to, or disclosure of Personal Data to a person, entity or system located in a country or jurisdiction other than the country or jurisdiction where the Personal Data originated from.

1.28 "UK Data Protection Law" shall mean all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (DPA 2018); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which applies to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which apply to a party.

1.29 "UK GDPR" shall have the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.30 "UK International Data Transfer Agreement" (IDTA) shall mean the standalone international data transfer agreement or the international data transfer addendum to the EU SCC (as applicable) issued by the UK Information Commissioner's Office under Section 119A of the DPA 2018 and which came into force on 21 March 2022, in replacement of the UK standard contractual clauses for transfers of UK personal data to a location outside of the UK.

1.31 "U.S. Data Protection Law" shall mean all applicable data protection and privacy legislation in force from time to time in the U.S., including without limitation, the CCPA, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Nevada online privacy law, the Texas Data Privacy and Security Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act.

2. Processing of Data

2.1 The rights and obligations of the Controller with respect to the Processing of the Controller Personal Information are described herein. Controller shall, in its use of the Services, always Process Personal Data and/or Personal Information (as applicable) and provide instructions for the Processing by Processor of the Controller Personal Information, in compliance with Data Protection Laws. The Parties agree that the Agreement and this Addendum constitute the Controller's complete and final documented instructions to Processor in relation to the Processing of the Controller Personal Information. Additional instructions outside the scope of the Agreement or this Addendum (if any) require a prior written agreement between Processor and Controller. Controller shall ensure that its instructions comply with all Data Protection Laws and that the Processing of the Controller Personal Information in accordance with Controller's instructions will not cause Processor to be in breach of Data Protection Laws. Controller is solely responsible for the accuracy, quality, and legality of (i) the Controller Personal Information provided to Processor by or on behalf of Controller, (ii) the means by which Controller acquired any such Controller Personal Information, and (iii) the instructions it provides to Processor regarding the Processing of such Controller Personal Information. Controller shall not provide or make available to Processor any Personal Data and/or Personal Information (as applicable) in violation of the Agreement or otherwise inappropriate for the nature of the Services. and shall defend, indemnify, and hold Processor harmless from and against all claims and losses in connection therewith.

2.2 Processor shall immediately notify Controller if an instruction, in the Processor's opinion, infringes the Data Protection Laws.

2.3 Controller agrees that (i) it will comply with its obligations under Data Protection Laws in respect of its Processing of the Customer Personal Information, including any obligations specific to its role as a Controller/Business and/or Processor/Service Provider (as applicable); and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Data Protection Laws for Processor to Process the Customer Personal Information including Processing of EU, Swiss and UK Personal Data in a location outside of the UK and EEA (as applicable) or the Personal Information of Canadian residents outside Canada (as applicable), as required to provide the Services pursuant to the Agreement and this Addendum. If Controller is itself a Processor/Service Provider with respect to the Controller Personal Information, Controller warrants to Processor that Controller's instructions and actions with respect to that Controller Personal Information, including its appointment of Qorus as another Processor or Service Provider (as applicable) have been authorized by the relevant Controller or Business (as applicable) under applicable Data Protection Laws.

2.4 Processor shall not Process the Controller Personal Information (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this Addendum or any other documented instructions provided by Controller, including with regard to Transfers of Personal Data to a third country or an international organization unless required to do so by a Supervisory Authority to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest and (iii) in violation of EU, Swiss, or UK Data Protection Laws (as applicable). Controller hereby instructs Processor to Process the Controller Personal Information in accordance with the foregoing and as part of any Processing initiated by Controller in its use of the Services.

2.5 For Personal Information that is subject to the CCPA, Processor acknowledges that it is prohibited from: (i) selling or sharing such Personal Information; (ii) retaining, using, or disclosing such Personal Information for a commercial purpose other than providing the Services or as otherwise permitted by the CCPA; (iii) retaining, using, or disclosing such Personal Information outside of the Agreement or other direct business relationship between Controller and Processor; and (iv) unless used for a business purpose that does not involve cross-context behavioural advertising and is permitted under eventual CPRA regulations, combining the Personal Information with personal information that Processor (a) receives from, or on behalf of, another person or persons; or (b) collects from its own consumer interaction.

2.6 this Processing, as well as the types of Controller Personal Information collected and the categories of Data Subjects, are described in Exhibit A to this Addendum.

2.7 Notwithstanding the foregoing, Processor may Process some Customer Personal Information for its own Legitimate Business Purposes, as an independent Controller, solely when the Processing is strictly necessary and proportionate, and if the Processing is for one of the following exhaustive list of purposes: (a) directly identifiable data (job title, name, email address, phone number, technical usage data) may be Processed for: (i) billing, account, and customer relationship management (marketing communication with procurement/sales employees of Controller), and related customer correspondence (mailings about for example necessary updates); (ii) complying with and resolving legal obligations, including responding to Data Subject Requests for Personal Data and/or Personal Information processed by Processor as a Controller (for example Website data), tax requirements, agreements and disputes; (iii) abuse detection prevention and protection, virus scanning and scanning to detect violations of terms of service (such as copyright infringement, SPAM, and actions not permitted under Processor's Terms of Use; (b) pseudonymized and/or aggregated data (Processor will pseudonymize and/or aggregate as much as possible and pseudonymized and/or aggregated data will not be processed on a per-customer level); for: (i) improving and optimizing the performance and core functionalities of accessibility, privacy, security, and the IT infrastructure efficiency of the Services and Website; (ii) internal reporting, financial reporting, revenue planning, capacity planning, and forecast modeling (including product strategy); (iii) receiving and using feedback for Processor's overall service improvement; and (iv) when acting as an independent Controller/Business, Processor will not process Customer Personal Information for any purposes other than the above list of Legitimate Business Purposes; or as provided in Section 2.8 below.

2.8 Processor may (a) derive and compile from the provision of the Services certain de-identified, aggregate and/or analytical data, which shall not contain any customer-specific or any individually identifying information ("Generic Data"), and (b) use Generic Data for

Processor's own purposes and without restriction, including but not limited to for use in conjunction with data from other sources to improve Processor's products and services and create new data models and products.

2.9 Except for Controller Personal Information which Processor may Process as a Controller under Sections 2.7 and 2.8 above, following completion of the Services, at Controller's choice, Processor shall return or delete the Controller Personal Information, unless further storage of the Controller Personal Information is required or authorized by applicable law. Data will be archived upon the termination of service and deleted within 90 days. If return or destruction is impracticable or prohibited by law, rule, or regulation, Processor shall take measures to block such Controller Personal Information from any further Processing (except to the extent necessary for its continued hosting or Processing required by law, rule, or regulation) and shall continue to appropriately protect the Controller Personal Information remaining in its possession, custody, or control. If Controller and Processor have entered into SCC and/or UK IDTA (as applicable), as described in Section 6 (Transfers of Personal Data), the Parties agree that the certification of deletion of the Controller Personal Information that is described in Clause 8.5 of the SCC shall be provided by Processor to Controller only upon Controller's request.

3. Authorized Employees

3.1 Processor shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorized Employee.

3.2 Processor shall ensure that all Authorized Employees are made aware of the confidential nature of Personal Data and Personal Information and have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement with Processor, any Personal Data and Personal Information except in accordance with their obligations in connection with the Services.

3.3 Processor shall take commercially reasonable steps to limit access to Personal Data and Personal Information to only Authorized Employees.

4. Authorized Sub-Processors

4.1 Controller acknowledges and agrees that Processor may (1) engage its affiliates and Authorized Sub-Processors to access and Process the Controller Personal Information in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the Processing of the Controller Personal Information. By way of this Addendum, Controller provides general written authorization to Processor to engage sub-processors as necessary to perform the Services. If and to the extent that the personal information Processed by the Authorized Sub-Processors qualifies as Personal Information under the CCPA, any such Authorized Sub-Processors used must qualify as a Service Provider under the CCPA and the Processor cannot make any disclosures to the Authorized Sub-Processors that the CCPA would treat as a sale.

A list of the Processor's current Authorized Sub-Processors (the "List") is available at https://www.qorusdocs.com/subprocessors/.

4.2 This List may be updated by Processor from time to time. Processor shall notify Controller of any new sub-processor Processor wishes to appoint to carry out Processing activities on behalf of Controller. Controller may reasonably object to such an engagement on legitimate grounds by informing Processor in writing within ten (10) days of receipt of the aforementioned notice by Controller. Controller acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Processor from offering the Services to Controller.

4.3 If Controller reasonably objects to an engagement in accordance with Section 4.2, and Processor cannot provide a commercially reasonable alternative within a reasonable period of time, Processor may terminate this Addendum. Termination shall not relieve Controller of any fees owed to Processor under the Agreement.

4.4 If Controller does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Processor, that third party will be deemed an Authorized Sub-Processor for the purposes of this Addendum.

4.5 Processor will implement policies requiring all Authorized Sub-Processors to comply with the data protection obligations comparable to those imposed on Processor under this Addendum with respect to the protection of Personal Data and Personal Information. Processor will annually review the Authorized Sub-Processor's IT governance policies and procedures. Processor will engage with the Authorized Sub-Processor to address any issues identified as a part of the review.

4.6 If Controller and Processor have entered into SCC and/or IDTA (as applicable), as described in Section 6 (Transfers of Personal Data), the above authorizations will constitute Controller's prior written consent to the Transfer of the Controller Personal Information to any Authorized Sub-Processors.

4.7 Notwithstanding any approval by Controller within the meaning of this Section 4, Processor shall remain fully liable vis-à-vis Controller for the performance of any such Authorized Sub-Processor that fails to fulfil its data protection obligations under this Addendum and/or any applicable Data Protection Laws.

5. Security of Personal Data.

5.1 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, Processor shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data and/or Personal Information (as applicable).

A summary of technical and organizational controls is available at https://www.qorusdocs.com/securitymeasures/.

5.2 Controller is responsible for reviewing the information made available by Processor relating to data security and making an independent determination as to whether the technical and organizational measures implemented by Processor meet Controller's requirements and legal obligations under Data Protection Laws. Controller acknowledges that Processor's technical and organizational measures are subject to technical progress and further development and that Processor may update or modify Processor's technical and organizational measures from time to time provided that such updates and modifications do not result in a material degradation of the overall security of the Services provided to Controller under the Agreement.

5.3 Controller agrees that without prejudice to Processor's obligations under Section 5.1: (a) Controller is responsible for its use of the Services, including making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Controller Personal Information, securing its account authentication credentials, managing its data back-up strategies, and protecting the security of the Controller Personal Information when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Personal Information uploaded to the Services; and (b) Processor has no obligation to protect the Controller Personal Information that Controller elects to store or transfer outside of Processor's and its Authorized Sub-Processors' systems (for example, offline or on-premise storage).

6. Transfers of Personal Data

6.1 The Parties agree that Processor may Process the Controller Personal Information outside the European Economic Area ("EEA"), the United Kingdom, or Switzerland, as necessary to provide the Services. If Processor transfers the Controller Personal Information to a jurisdiction for which the European Commission or the UK Government, as applicable, has not issued an adequate decision, Processor will ensure that appropriate safeguards have been implemented for the Transfer of the Controller Personal Information in accordance with applicable Data Protection Laws.

6.2 Where required, any Transfer of the Controller Personal Information to any countries which do not ensure an adequate level of data protection shall be undertaken by Processor in accordance with the SCC and/or the IDTA, as applicable. For the purposes of this Section 6.2, Processor and Controller hereby agree to enter into the SCC and/or IDTA, subject to the following:

6.2.1 The Standard Contractual Clauses approved by the European Commission in its Decision of 4 June 2021 (2021/914) with Module Two (*Transfer Controller to Processor*) selected ("**C2P SCCs**"), are incorporated herein by reference and apply to all transfers of Customer Personal Information by or on behalf of Controller to Processor or any Authorized Sub-processor where:

(i) Clause 7 ("Docking clause") shall not apply.

(ii) Option 2 ("General Written Authorization") of Clause 9(a) ("Use of sub-processors") shall apply.

(iii) The optional language in Clause 11(a) ("Redress") shall not apply.

(iv) Option 1 of Clause 17 ("Governing Law") shall apply, and the applicable law shall be the law of France.

(v) In Clause 18 ("Choice of forum and jurisdiction") the applicable courts shall be the courts of France.

(vi) The list of parties and description of the Transfer in Annex I of the Clauses shall be as described in Exhibit A to this Addendum.

(vii) The competent supervisory authority shall be the Commission Nationale de l'Informatique et des Libertés; and

(viii) The technical and organizational measures of the Clauses shall be as described in Exhibit B of this Addendum.

6.2.2 For the purposes of the Swiss Data Protection Law, the SCCs shall apply with the following amendments:

(i) In Clause 2, the words: "and, with respect to data transfers from controller to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679" shall be deleted;

(ii) Clause 8.8(i) is replaced with: "the onward transfer is to a country that has been the subject of an adequacy assessment by the FDPIC or the Federal Council (as the case may be) that covers the onward transfer";

(iii) 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 or "GDPR")" are to be interpreted as references to the nDPA to the extent applicable;

(iv) References to "Regulation (EU) 2018/1725" are removed;

(v) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" shall be interpreted to mean Switzerland;

(vi) Clause 13 (a) and Part C of Annex I are not used;

(vii) The "competent supervisory authority" and "supervisory authority" are both replaced with the FDPIC insofar as the transfers are governed by the nDPA;

(viii) In Clause 16(e), subsection (i) is replaced with: "the FDPIC adopts its own standard contractual clauses pursuant to Article 16(2)(d) of the n DPA that cover the transfer of personal data to which these clauses apply";

(ix) Clause 17 is replaced with: "These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by the nDPA.";

(x) Clause 18 is replaced with: "Any dispute arising from these Clauses relating to the nDPA shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which they have their habitual residence. The parties agree to submit themselves to the jurisdiction of such courts.";

(xi) As long as the DPA is in force, the EU SCC shall also protect Personal Data of legal entities and legal entities shall receive the same protection under the EU SCC as natural persons.

6.2.3 To the extent that Processor Processes as a Processor any Customer Personal Information that originates from the United Kingdom in a country that has not been designated by the UK Secretary of State as providing an adequate level of protection for Personal Data, Processor shall also enter into an IDTA with Controller in the form that can be accessed at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/

Where applicable, the signed IDTA shall form an integral part of this Addendum as if fully set forth herein. The information required by Appendix 1 and Appendix 2 to the IDTA is set forth in Exhibit A hereto.

6.3 To the extent that Controller or Processor are relying on a specific statutory mechanism to normalize Transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, Controller and Processor agree to cooperate in good faith to promptly terminate the Transfer or to pursue a suitable alternative mechanism that can lawfully support the Transfer.

7. Rights of Data Subjects

7.1 Processor shall, to the extent permitted by Data Protection Laws, promptly notify Controller upon receipt of a complaint, dispute or request it has received from a Data Subject or a consumer under CCPA to exercise the Data Subject's or consumer's right of access, rectification, erasure, data portability, restriction or cessation of Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Processor receives a Data Subject Request in relation to Controller's data, Processor will advise the Data Subject or CCPA consumer (as applicable) to submit their request to Controller, and the Controller will be responsible for responding to such request, including, where necessary, by making a request to the QorusDocs help center. Controller is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of Processing, or withdrawal of consent to Processing of any Controller Personal Information are communicated to Processor, and for ensuring that a record of consent to Processing is maintained with respect to each Data Subject and/or CCPA consumer (as applicable).

7.2 Processor shall, at the request of the Controller, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Controller in complying with Controller's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Controller is itself unable to respond without Processor's assistance and (ii) Processor is able to do so in accordance with all applicable laws, rules, and regulations. Controller shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Processor.

7.3 Controller agrees that, without prejudice to Processor's obligations under Sections 7.1 and 7.2 above, Controller is solely responsible for dealing with Data Subject Requests.

7.4 If a law enforcement agency sends Processor a demand for Controller Personal Information (e.g., a subpoena or court order), Processor will redirect the law enforcement agency to request that data directly from Controller. As part of this effort, Processor may provide Controller's contact information to the law enforcement agency. If compelled to disclose Controller Personal Information to a law enforcement agency, then Processor will give Controller reasonable notice of the demand to allow Controller to seek a protective order or other appropriate remedy to the extent possible and if Processor is legally permitted to do so.

7.5 Controller acknowledges that Processor is required under EU and UK Data Protection Law to: (a) collect and maintain written records of certain information, including the name and contact details of each Processor and/or Controller on behalf of which Processor is acting and, where applicable, of such Processor's or Controller's local representative and data protection officer. and (b) make such information available to the Supervisory Authorities. Accordingly, if EU and/or UK Data Protection Law applies to the Processing of the Controller's Personal Data, Controller will, where requested, provide such information to Processor via the Services or other means provided by Processor, and will ensure that all information provided is kept accurate and up to date.

8. Cooperation. Audits. Personal Data Breach.

8.1 Processor shall, taking into account the nature of the Processing and the information available to Processor, provide Controller with reasonable cooperation and assistance where necessary for Controller to comply with its obligations under applicable Data Protection Laws to conduct a data protection impact assessment, or with respect to Controller's cooperation and/or prior consultation with any Supervisory Authority, *provided that* Controller does not otherwise have access to the relevant information. Controller shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Processor.

8.2 Controller acknowledges that Processor is regularly audited by independent third-party auditors and/or internal auditors against the standards specified in the Qorus Security Standards, as described in Exhibit B. Upon Controller's request, Processor shall, no more than once per calendar year, either (i) make available for Controller's review copies of certifications or reports demonstrating Processor's compliance with such standards, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Controller or its authorized representative, upon reasonable notice and at a mutually agreeable date and time, to conduct an audit or inspection of Processor's data security infrastructure and procedures that are sufficient to demonstrate Processor's compliance with its obligations under this Addendum, provided that such inspection shall not be unreasonably disruptive to Processor's business. Controller shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Processor for any time expended for on-site audits. If Controller and Processor have entered into SCCs and/or an IDTA as described in Section 6 (Transfers of Personal Data), the Parties agree that the audits described in Clauses 8.9(c)-(d) of the SCC shall be carried out in accordance with this Section 8.2.

8.3 In the event of a Personal Data Breach that impacts the Processing of the Customer Personal Information and is reasonably likely to require a data breach notification by Controller under applicable Data Protection laws, Processor shall, without undue delay, inform Controller of the Personal Data Breach and take such steps as Processor in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Processor's reasonable control).

8.4 In the event of a Personal Data Breach, Processor shall, taking into account the nature of the Processing, the information available to Processor, and any restrictions on disclosing such information, such as confidentiality, provide Controller with reasonable cooperation and assistance necessary for Controller to comply with its obligations under applicable Data Protection Laws with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.5 Controller agrees that an unsuccessful Personal Data Breach will not be subject to this Section 8. An unsuccessful Personal Data Breach results in no unauthorized access to the Controller Personal Information or any of Processor's equipment or facilities storing the Controller Personal Information and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar events.

8.6 Controller acknowledges that Processor will not assess the contents of the Controller Personal Information in order to identify information subject to any specific legal requirements. Controller is solely responsible for complying with the data breach notification obligations applicable to Controller under Data Protection Laws and fulfilling any third-party notification obligations related to any Personal Data Breach.

8.7 The obligations described in Sections 8.6 and 8.7 shall not apply if a Personal Data Breach results from the actions or omissions of the Controller. Processor's obligation to report or respond to a Personal Data Breach under Section 8.3 will not be construed as an acknowledgment by Processor of any fault or liability with respect to the Personal Data Breach.

9. CCPA Warranties

9.1 Both parties will comply with all applicable requirements of the CCPA when collecting, using, retaining, or disclosing Personal Information.

9.2 Processor warrants that it has no reason to believe any CCPA requirements or restrictions prevent it from providing any of the Contracted Business Purposes or otherwise performing its obligations under this Addendum. Processor must promptly notify Controller of any changes to the CCPA's requirements that may adversely affect its performance under the Agreement.

10. Limitation of Liability

The total liability of each of Controller and Processor (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this Addendum, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement. Controller agrees that any regulatory penalties incurred by Processor in relation to the Processing of the Controller Personal Data that arise as a result of, or in connection with, Controller's failure to comply with its obligations under this Addendum and Data Protection Laws shall count towards and reduce Processor's liability under the Agreement as if it were a liability to Controller under the Agreement.

11. General Provisions. Governing Law and Choice of Forum and Jurisdiction

11.1 General

(a) If any provision of this Addendum is ineffective or void, this shall not affect the remaining provisions. The parties shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. In case a necessary provision is missing, the Parties shall add an appropriate one in good faith.

(b) In the event of any inconsistency between the provisions of this Addendum and the provisions of the Agreement, the provisions of this Addendum shall prevail.

11.2 Governing Law

(a) This Addendum (insofar as relates to any EU Personal Data, if any, being Processed hereunder) and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Addendum (only insofar as relates to EU Personal data being Processed hereunder) shall be governed by and construed in accordance with the laws of France.

(b) This Addendum (insofar as relates to any UK Personal Data, if any, being Processed hereunder), and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Addendum (only insofar as relates to UK Personal Data being Processed hereunder) shall be governed by and construed in accordance with the law of England and Wales.

(c) This Addendum (insofar as relates to any Swiss Personal Data, if any, being Processed hereunder) and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Addendum (only insofar as relates to Swiss Personal Data being Processed hereunder), shall be governed by and construed in accordance with the laws of Switzerland.

(d) This Addendum (insofar as relates to any other Personal Data and/or Personal Information being Processed hereunder) and all matters arising out of or relating to this DPA, whether sounding in contract, tort, or statute, shall be governed by and construed in accordance with the laws of the State of Washington, without giving effect to the conflict of laws provisions thereof to the extent such principles or rules would require or permit the application of the laws of any jurisdiction other than those of the State of Washington.

11.3 Forum and Jurisdiction

(a) Each party irrevocably agrees that the courts of France shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with the processing of any EU Personal Data under this Addendum.

(b) Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with the processing of any UK Personal Data under this Addendum.

(c) Each party irrevocably agrees that the courts of Switzerland shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with the processing of any Swiss Personal Data under this Addendum.

(d) Each Party irrevocably and unconditionally agrees that it will not commence any action, litigation, or proceeding of any kind whatsoever against the other Party in any way arising from or relating to any Processing of any other Personal Data and/or Personal Information under this Addendum, including, but not limited to, contract, equity, tort, fraud, and statutory claims, in any forum other than the courts of the State of Washington and any appellate court from any thereof. Each Party irrevocably and unconditionally submits to the exclusive jurisdiction of such courts and agrees to bring any such action, litigation, or proceeding only in the courts of the State of Washington. Each Party agrees that a final judgment in any such action, litigation, or proceeding is conclusive and may be enforced in other jurisdictions by suit on the judgment or in any other manner provided by law.

EXHIBIT A
Details of Processing

A. LIST OF PARTIES

Data exporter(s):

The entity that has entered into the Agreement with data importer for the provision of the products and services as described in the Agreement and/or applicable order form.

Activities relevant to the data transferred under these Clauses: Uploading, transmiting, and otherwise processing the data through products or services of Processor.

Role: Controller

Data importer(s):

1. Name: Qorus Software Inc.

Address: 3120 139th Ave SE, Suite 500, Bellevue, WA, 98005

Contact person’s name, position and contact details: Stéphanie Laurent, CTO, Security@qorusdocs.com

Activities relevant to the data transferred and Processed under these Clauses:

> QorusDocs displays the logged-in user’s First Name, Last Name, and Profile Picture on the User Interface to greet them after successful sign-in.
>
> The user’s First Name, Last Name, Region, Time Zone, Corporate Email Address, and Profile Picture are displayed to other users to work collaboratively.
>
> The user’s Corporate Email Address is used to send emails to the user related to particular tasks that other users are expecting them to do as part of the software.
>
> Content created with QorusDocs may contain user data, the extent of which is solely determined and controlled by the Data Exporter.
>
> Pursuits, Smart Fields, and Smart Lists, or other functionality may contain user data, the extent of which is solely determined and controlled by the Data Exporter.
>
> Should the Data Exporter personnel share content with customers and prospects, their corporate email address shall be transferred.

B. DESCRIPTION OF TRANSFER

Description of transfer between the data exporter and data importer:

Description	**Details**
Categories of data subjects whose personal data is transferred	The data exporter will submit personal data to the Service, the extent of which will be determined and controlled by the data exporter in the data exporter's sole discretion, and which may include personal data relating to the following categories of data subjects: • the data exporter's officers, employees, contractors (Personnel) who are natural persons • the data exporter's customers, prospects who are natural persons
Categories of personal data transferred	The data exporter will submit personal data to the Service, the extent of which will be determined and controlled by the data exporter in the data exporter's sole discretion. Personal data Processed by the Service includes the following categories of personal data: • for the data exporter's Personnel: First name Last name, Corporate email address, Country of residence, and time zone. At the Data Exporter's discretion, personal data Processed by the Service may include the following categories of personal data: • for the data exporter's customers and prospects: o Content created with Qorus may contain prospect/customer personal data, the extent of which is solely determined and controlled by the data exporter. Should the data exporter personnel share content with customers and prospects, their corporate email address shall be transferred. When electing to use QorusDocs AI, users may submit personal or other types of data to the Service, the extent of which will be determined and controlled by the data exporter in the data exporter's sole discretion. • Prompts are submitted by the user and stored as entered by the user in the QorusDocs Azure SQL database. • When users elect to index content to be used as part of the functionality, the documents text content is stored in QorusDocs database and a vectorial representation of the text content of the document is stored in Pinecone.
Sensitive data transferred	None
The frequency of the transfer	Subject to the terms in the Addendum, the Processing will occur for the duration of the Agreement, unless otherwise agreed upon between the data exporter and the data importer in writing.
Nature of the processing	QorusDocs enable users to perform the following functions: • Retrieval of personal data • Storage of personal data.
Purpose(s) of the data transfer and further processing	QorusDocs enables users to create documents such as proposals, RFPs, pitches, presentations, security questionnaires, and statements of work.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Data is retained for the period of the Agreement plus 90 days.

CCPA Categories

Personal Information Categories: This Addendum may involve, at Controller's discretion, the following types of Personal Information, as defined and classified in CCPA Cal. Civ. Code § 1798.140(o), as amended by the CPRA.

Category	Personal Information
A. Identifiers.	A real name, alias, postal address, unique personal identifier, email address, account name, or other similar identifiers.
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, address, telephone number. Some personal information included in this category may overlap with other categories.
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

When electing to use QorusDocs AI, users may submit personal or other types of data to the Service, the extent of which will be determined and controlled by the data exporter in the data exporter's sole discretion.

- Prompts are submitted by the user and stored as entered by the user in the QorusDocs Azure SQL database.
- When users elect to index content to be used as part of the functionality, the documents text content is stored in QorusDocs database and a vectorial representation of the text content of the document is stored in Pinecone.

Authorized Sub-Processors:

A list of Authorized Sub-Processors may be found at https://www.qorusdocs.com/subprocessors/.

Technical and Organizational Measures:

A summary of technical and organizational controls is available at https://www.qorusdocs.com/securitymeasures/.

Controller

Signature:____________________________________

Customer Legal Name:__________________________

Print Name:__________________________________

Title:______________________________________

Date:___________________________________

Processor

Signature:____________________________________

Print Name:__________________________________

Title:______________________________________

Date:______________________________________