# QLIK® CUSTOMER AGREEMENT

## I. GENERAL TERMS

**1. Agreement.** This Agreement is between Customer and the Qlik entity identified on an Order Form or in Table 1 to this Agreement ("Qlik") and governs the use of all Qlik Products and Services accessed or used by Customer.

### 2. Definitions

Unless defined elsewhere in this Agreement, the capitalized terms utilized in this Agreement are defined below.

**2.1.** "**Agreement**" means this Qlik Customer Agreement, each addendum attached hereto (which is incorporated by reference), and any Order Form(s) between Qlik and Customer for the provision of Qlik Products or Services.

**2.2.** "**Authorized Third Party**" means any third party authorized by Customer to access and use any Qlik Products, designated for external use in the Documentation or Order Form, provided such use is solely in connection with Customer's business relationship with the authorized third party.

**2.3.** "**Authorized Reseller**" means a reseller, distributor or other third party authorized by Qlik to sell Qlik Products or Services.

**2.4.** "**Authorized User**" means (a) in the case of an individual accepting this Agreement on such individual's own behalf, such individual; or (b) an employee, contractor, consultant or Authorized Third Party of Customer, who has been authorized by Customer to use the Qlik Products in accordance with the terms and conditions of this Agreement and has been allocated a license or user credentials.

**2.5.** "**Confidential Information**" means non-public information that is disclosed by or on behalf of a Party under or in relation to this Agreement that is identified as confidential at the time of disclosure or should be reasonably understood to be confidential or proprietary due to the nature of the information and/or the circumstances surrounding its disclosure. Confidential Information does not include information which, and solely to the extent it: (i) is generally available to the public other than as a result of a disclosure by the receiving Party or any of its representatives; (ii) was known or becomes known to the receiving Party from a source other than disclosing Party or its representatives without having violated any confidentiality agreement of the disclosing Party; (iii) is independently developed by the receiving Party without the use or benefit of any of the disclosing Party's Confidential Information; or (iv) was disclosed by the disclosing Party to a third party without an obligation of confidence. In any dispute concerning the applicability of these exclusions, the burden of proof will be on the receiving Party and such proof will be by clear and convincing evidence.

**2.6.** "**Consulting Services**" means any consulting services for Qlik Products performed by Qlik under the terms of this Agreement and any applicable Order Form.

**2.7.** "**Content**" means information, data, materials, media or other content provided by or on behalf of Customer and/or its Authorized Users for use with Qlik Products or Services, including data from third party applications enabled by Customer or an Authorized User. Content may also be referred to as Customer Data.

**2.8.** "**Customer**" means an individual or company that has entered into this Agreement by electronically accepting the terms or by accessing or using the Qlik Products; or where an Order Form has been executed, then Customer means the entity identified on the Order Form.

**2.9.** "**Delivery Date**" means the date on which access to the Qlik Products is initially made available (via download or otherwise) to Customer or to the Authorized Reseller as applicable, which date may be specified in an Order Form.

**2.10.** "**Documentation**" means the then-current technical and user documentation for the Qlik Products, including the applicable product descriptions and/or service description guide available at www.qlik.com/product-terms.

**2.11.** "**Education Services**" means any training or education services performed by Qlik, including educational content provided by Qlik online or by an instructor, under the terms of this Agreement and any applicable Order Form.

**2.12.** "**Export Control Laws**" means export control laws and regulations of the U.S., E.U., and other governments, as well as regulations and sanctions declared by the U.S. Department of the Treasury Office of Foreign Assets Control, the U.S. Department of Commerce, the Council of the E.U. and their counterparts under applicable law, including all end user, end use and destination restrictions.

**2.13.** "**IP Claim**" means a claim brought by a third party alleging that the Qlik Products, as delivered by Qlik and used as authorized under this Agreement, infringes upon any third- party copyright, trademark or a patent.

**2.14.** "**Order Form**" means an order form, statement of work or written document pursuant to which Customer orders Qlik Products or Services that is executed by the Parties, or executed by Customer and an Authorized Reseller.

**2.15.** "**Party**" or "**Parties**" means Qlik and Customer, individually and collectively, as the case may be.

**2.16.** "**Qlik Acceptable Use Policy**" means Qlik's then current Qlik Cloud Acceptable Use Policy located at www.qlik.com/product-terms.

**2.17.** "**Qlik Cloud**" means any subscription-based, SaaS solution provided and managed by Qlik or its affiliate.

**2.18.** "**Qlik Cloud Client**" means a software client that must be downloaded and installed to use Qlik Cloud.

**2.19.** "**Qlik Marks**" means Qlik's trademarks, service marks, trade names, logos, and designs, relating to Qlik Products, whether or not specifically recognized, registered or perfected, including without limitation, those listed on Qlik's website.

**2.20.** "**Qlik Products**" means Software and Qlik Cloud products provided by Qlik and its affiliates. Qlik Products do not include Services or early release, beta versions or technical previews of product offerings.

**2.21.** "**Services**" means Support, Consulting Services or Education Services performed by Qlik under the terms of this Agreement and any applicable Order Form. Services does not include Qlik Cloud.

**2.22.** "**Software**" means the generally available release of the Qlik software made available under this Agreement, in object code form, initially provided or made available to Customer as well as updates thereto that Qlik elects to make available at no additional charge to all of its customers that subscribe to Support for the Software.

**2.23.** "**Support**" means end user support and access to updates for the Qlik Products, which are provided by Qlik as part of a paid subscription or support contract.

## 3. Customer Rights and Responsibilities

**3.1. Provision of Qlik Products.** Subject to the terms of this Agreement, Qlik grants to Customer a world-wide, nonexclusive, non-transferable and non-sublicensable right for its Authorized Users to access or use Qlik Products for Customer's internal business operations, provided any use of Qlik Products shall be: (i) in accordance with the Documentation and this Agreement; and (ii) for the scope, term and quantities which may be specified in an Order Form.

**3.2. Services.** Support for Software will be provided in accordance with Qlik's Support Policy, and for Qlik Cloud, in accordance with Qlik's Service Level Agreement. Notwithstanding the above, support for any Talend-branded products will be provided in accordance with the Talend Service Description Guide. The applicable Support terms are attached hereto and available at www.qlik.com/product-terms. Qlik may provide Consulting or Education Services to Customer pursuant to this Agreement, any applicable product descriptions attached hereto and (available at www.qlik.com/product-terms) and any applicable Order Form.

**3.3. Consulting and Education Warranty**. Qlik warrants that Consulting Services and Education Services will be performed using reasonable care and skill consistent with generally accepted industry standards. For any claimed breach of this warranty, Customer must notify Qlik of the warranty claim within thirty (30) days of Customer's receipt of the applicable Consulting Services or Education Services. Customer's exclusive remedy and Qlik's sole liability with regard to any breach of this warranty will be, at Qlik's option and expense, to either: (i) re-perform the non-conforming Consulting Services or Education Services; or (ii) refund to Customer the fees paid for the non-conforming Consulting Services or Education Services. Customer shall provide reasonable assistance to Qlik in support of its efforts to furnish a remedy for any breach of this warranty.

**3.4. Use Restrictions.** Except as expressly permitted by this Agreement, Customer will not, nor permit or authorize anyone to:

**3.4.1.** distribute, convey, lend, lease, share, sell, transfer, sublicense, rent, or time share any of the Qlik Products, or any of its components or product keys, or permit third parties to download or install any Software;

**3.4.2.** copy, decompile, disassemble or reverse engineer or otherwise attempt to extract or derive the source code or any methods, algorithms or procedures from the Qlik Products, except as otherwise expressly permitted by applicable law, or modify, adapt, translate or create derivative works based upon the Qlik Products;

**3.4.3.** alter or circumvent any product, key or license restrictions, or transfer or reassign a named user license or entitlement, in such a manner that enables Customer to exceed purchased quantities, defeat any use restrictions, or allows multiple users to share such entitlement to exceed purchased quantities;

**3.4.4.** use, offer, embed, or otherwise exploit the Qlik Products, whether or not for a fee, in any managed service provider (MSP) offering; platform as a service or integration platform as a service (PaaS or iPaaS) offering; service bureau; or other similar product or offering, including offering standalone Qlik Products as a hosted service;

**3.4.5.** use the Qlik Products if Customer is a competitor, or use the Qlik Products in any manner that competes with Qlik, including but not limited to, benchmarking, collecting and publishing data or analysis relating to the performance of the Qlik Products, or developing or marketing a product that is competitive with any Qlik Product or service;

**3.4.6.** use the Qlik Products in any manner or for any purpose that infringes, misappropriates or otherwise violates any intellectual property right or other right of any third party or that violates any applicable law; or

**3.4.7.** interfere with or disrupt the integrity, operation, or performance of the Qlik Products or interfere with the use or enjoyment of it by others.

**3.4.8.** use a Qlik Cloud Client for any purpose other than to access or use Qlik Cloud in accordance with this Agreement.

**3.5. Qlik Marks.** For so long as Customer has the right to access and use Qlik Products, Qlik grants to Customer a nonexclusive, non-transferable and limited right to use Qlik Marks for the sole purpose of promoting any permitted use of Qlik Products. Any use of Qlik Marks must be in compliance with the Qlik Logo and Trademark Policy available at www.qlik.com. Customer may not remove or obscure any copyright, trademark or other proprietary notice displayed or included in the Qlik Products.

**3.6. Use.** Customer shall ensure that use of Qlik Products and Services is at all times compliant with this Agreement and all applicable laws, including any Export Control Laws. Customer is solely responsible for compliance relating to the manner and purpose in which it chooses to use Qlik Products, including but not limited to, the transfer and processing of Content, the provision of Content to end users, and any industry specific requirements to which Customer may be subject.

**3.7. Access**. Customer is solely and directly responsible (a) for maintaining the security of all keys, user IDs, passwords and other credentials, (b) for all acts and omissions taken by its Authorized Users or under any of its keys or credentials; and (c) to promptly notify Qlik of any unauthorized use or access and take all steps necessary to terminate such unauthorized use or access. Customer will provide Qlik with such cooperation and assistance related to any unauthorized use or access as Qlik may reasonably request.

**3.8. Payment and Taxes**. Customer shall pay all fees due within thirty (30) days from the receipt date of Qlik's or its authorized reseller's valid invoice therefor, unless otherwise stated on an Order Form. Fees are not subject to any right of offset or suspension. Qlik shall state separately on invoices taxes excluded from the fees, and the [Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k). If the Customer fails to pay any Fee when due, then Qlik or its authorized reseller as applicable may charge Customer interest in an amount of interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid. In the event any use of Qlik Products exceeds purchased quantities ("Overage"), without limiting Qlik's other rights and remedies at law or in equity, Customer will be invoiced and shall pay for such Overage as specified in an Order Form.

**3.9. Billing Information**. Customer agrees to provide Qlik with accurate, timely and complete payment and invoicing information, including current contact information and tax identification numbers.

## 4. Intellectual Property Rights and Indemnification

**4.1. Ownership.** Customer retains all right, title and interest in and to all Content. Qlik retains all right, title and interest in and to the Qlik Products, Documentation and if applicable, all Education Services materials and Consulting Services deliverables, including all know-how, methodologies, designs and improvements to the Qlik Products, but excluding any Content incorporated into any such Services. Qlik hereby grants Customer a non-exclusive license to use any Education Services materials and Consulting Services deliverables or work product in connection with Customer's authorized use of the Qlik Products.

**4.2. Retention of Rights.** No title or ownership of any proprietary or other rights related to Qlik Products is transferred or sold to Customer or any Authorized User pursuant to this Agreement. All intellectual property rights not explicitly granted to Customer are reserved and Qlik, its affiliates, and their respective suppliers or licensors, where applicable, retain all right, title and interest in and to the Qlik Products, including all intellectual property rights embodied therein, as well as to all Qlik Marks. Customer is not obligated to provide Qlik with any suggestions or feedback about the Qlik Products, but if Customer elects to do so, Qlik may use and modify this feedback for any purpose, including developing and improving the Qlik Products, without any liability, time limitation, restriction, or payment to Customer.

**4.3. Indemnification.** Qlik shall have the right to intervene to defend, indemnify and hold Customer and its directors, officers, employees, agents, and permitted successors and assigns harmless from any damages and costs awarded against Customer and its directors, officers, employees, agents, successors and assigns as a result of an IP Claim. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

**4.4. Procedures.** Qlik's indemnification obligation is subject to: (i) Customer's prompt notification of a claim in writing to the Qlik; (ii) consent to allow Qlik to have sole control of the defense and any related settlement negotiations; and (iii) provision of information, authority and assistance as necessary for the defense and settlement of an indemnified claim. Qlik shall not consent to entry into judgment or enter into any settlement that admits liability Customer or provides for injunctive or other non-monetary relief affecting Customer, without the prior consent of Customer, which consent shall not be unreasonably withheld.

**4.5. Exceptions.** Qlik will not be liable for any IP Claim arising from or based upon: (i) any unauthorized use, reproduction or distribution of the Qlik Products; (ii) any modification or alteration of the Qlik Products without the prior written approval of Qlik; (iii) use of the Qlik Products in combination with any other software, hardware, third-party data or other materials not provided by Qlik or expressly authorized in the applicable Documentation; (iv) use of a prior version of the Qlik Product, if use of a newer version of the Qlik Product would have avoided such claim; or (v) any Third-Party Materials not used in accordance with the Documentation.

**4.6. Remedies.** If the Qlik Product becomes, or, in Qlik's opinion, is likely to become, the subject of an IP Claim, Qlik may, at its option and expense, either: (i) obtain the right for Customer to continue using the Qlik Product in accordance with this Agreement; (ii) replace or modify the Qlik Product so that it becomes non-infringing while retaining substantially similar functionality; or (iii) if neither of the foregoing remedies can be reasonably provided by Qlik, terminate all rights to use the Qlik Products (without need for a ruling by a court or arbitrator) and refund as applicable a pro rata portion of unused, prepaid fees.

**4.7. SOLE AND EXCLUSIVE REMEDY.** THIS SECTION 4 STATES QLIK'S SOLE AND ENTIRE OBLIGATION AND LIABILITY, AND CUSTOMER'S AND ITS AFFILIATES' SOLE AND EXCLUSIVE RIGHT AND REMEDY, FOR ANY CLAIM OF INFRINGEMENT OR ALLEGED VIOLATION OF INTELLECTUAL PROPERTY RIGHTS.

## 5. Limitation of Liability

**5.1. Limitation of Liability.** Except for: (i) Qlik's indemnification obligations under this Agreement, (ii) death or bodily injury caused by a Party's negligence; (iii) Customer's payment obligations; and (iv) Customer's violation of Qlik's intellectual property rights, each Party's maximum, cumulative liability for any claims, losses, costs (including attorney's fees) and other damages arising under or related to this Agreement, regardless of the form of action, whether in contract, tort (including negligence or strict liability) or otherwise, will be limited to actual damages incurred, and will in no event exceed the greater of the amount of fees paid or payable by Customer for the twelve (12) month period preceding the loss or damages giving rise to the claim and attributable to the specific products or services giving rise to such damages, or one thousand U.S. dollars (USD $1,000). THIS AGREEMENT SHALL NOT IMPAIR THE U.S. GOVERNMENT'S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF OR RELATED TO THIS CONTRACT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31 U.S.C. 3729-3733. FURTHERMORE, THIS CLAUSE SHALL NOT IMPAIR NOR PREJUDICE THE U.S. GOVERNMENT'S RIGHT TO EXPRESS REMEDIES PROVIDED IN THE GSA SCHEDULE CONTRACT (E.G., CLAUSE 552.238-75 – PRICE REDUCTIONS, CLAUSE 52.212-4(H) – PATENT INDEMNIFICATION, AND GSAR 552.215-72 – PRICE ADJUSTMENT – FAILURE TO PROVIDE ACCURATE INFORMATION).

**5.2. Exclusion of Damages.** EXCEPT FOR EITHER PARTY'S BREACH OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, IN NO EVENT SHALL EITHER PARTY BE LIABLE UNDER CONTRACT, TORT, STRICT LIABILITY, NEGLIGENCE, WARRANTY OR ANY OTHER LEGAL OR EQUITABLE THEORY WITH RESPECT TO THE SERVICES,INCLUDING FOR ANY LOST PROFITS, DATA OR CONTENT LOSS, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF GOODWILL, OR FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE, COMPENSATORY OR CONSEQUENTIAL DAMAGES OF ANY KIND WHATSOEVER, EVEN IF THE PARTY HAD BEEN ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES.

**5.3.** THE LIMITATIONS, EXCLUSIONS AND DISCLAIMERS CONTAINED IN THIS AGREEMENT ARE INDEPENDENT OF ANY AGREED REMEDY SPECIFIED IN THIS AGREEMENT AND WILL APPLY TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY AGREED REMEDY IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE. TO THE EXTENT THAT QLIK MAY NOT, AS A MATTER OF LAW, DISCLAIM ANY WARRANTY OR LIMIT ITS LIABILITIES, THE SCOPE OR DURATION OF SUCH WARRANTY AND THE EXTENT OF QLIK'S LIABILITY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. IF A WAIVER, RIGHT, OR REMEDY IS EXERCISED PURSUANT TO MANDATORY LAW, IT SHALL BE EXERCISED SOLELY FOR THE PURPOSE PROVIDED AND IN CONFORMANCE WITH THE PROCEDURES AND LIMITATIONS EXPRESSLY PROVIDED FOR BY SUCH LAW.

**5.4. No Third-Party Beneficiaries.** The warranties and other obligations of Qlik under this Agreement run only to, and for the sole benefit of Customer, notwithstanding any rights of Authorized Third Parties to access or use the Qlik Products. Except as otherwise mandated by applicable law, no person or entity will be considered a third-party beneficiary of this Agreement or otherwise entitled to receive or enforce any rights or remedies in relation to this Agreement.

**5.5. Warranty Disclaimer.** EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, QLIK MAKES NO OTHER WARRANTIES AND HEREBY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE (EVEN IF QLIK HAS BEEN INFORMED OF SUCH PURPOSE). QLIK DOES NOT WARRANT THAT THE QLIK PRODUCTS AND SERVICES WILL BE ERROR-FREE, COMPLETELY SECURE OR MEET CUSTOMER'S REQUIREMENTS.

## 6. Confidentiality

Each Party will hold in confidence the other Party's Confidential Information and will not disclose or use such Confidential Information except as necessary to exercise its express rights to perform its express obligations hereunder. Any Party's disclosure of the other Party's Confidential Information may be made only to those of its employees or consultants who need to know such information in connection herewith and who have agreed to maintain the Confidential Information as confidential as set forth herein. Notwithstanding the foregoing, a Party may disclose the other Party's Confidential Information to the extent that it is required to be disclosed in accordance with an order or requirement of a court, administrative agency or other governmental body, provided that such Party, to the extent permitted by law, provides the other Party with prompt notice of such order or requirement in order that it may seek a protective order. Each Party's confidentiality obligations hereunder will continue for a period of three (3) years following any termination of this Agreement, provided, however, that each Party's obligations will survive and continue in effect thereafter with respect to, and for so long as, any Confidential Information continues to be a trade secret under applicable law. Qlik recognizes that Customers may be subject to the Freedom of Information Act 5 U.S.C. 552 or other similar open records law which may require that certain information be released, despite being characterized as "confidential" by the vendor. The Parties acknowledge and agree that the Qlik Products and all pricing information are Confidential Information of Qlik.

## 7. Term and Termination

**7.1. Term.** This Agreement is effective upon the earlier of the effective date of the first Order Form referencing this Agreement or the date Customer is first provided with access to or use of the Qlik Products and shall remain in effect until expiration or termination of all rights to use any Qlik Products, which may be specified in any applicable Order Form. Subscriptions shall automatically terminate at the end of the then-current term unless a renewal is otherwise agreed to by the parties in writing. Except as otherwise set forth herein, subscriptions may not be cancelled in whole or in part during any subscription period.

**7.2. Termination for Breach.** The Customer may terminate this Agreement (without resort to court or other legal action) if Qlik fails to cure a material breach within thirty (30) days in accordance with FAR 51.212-4(m) or other similar law or regulation if applicable to the relevant Order Form.

**7.3**. **Termination for Cause**. Subject to 41 U.S.C. § 71 (Contract Disputes), FAR 52.233-1 (Disputes), applicable local law or regulation, and unless a remedy is otherwise ordered by a United States Federal Court, Qlik may terminate the Agreement if it is determined that the Customer failed to comply with the Terms. Customer may terminate the Agreement effective immediately upon written notice to Qlik if Qlik (A) fails to cure a breach of the Agreement within 30 days of notice of the breach, or (B) commits an uncurable material breach of the Agreement, or (C) terminates or suspend its business.

**7.4.** Qlik may terminate Customer's or any individual Authorized User's access to all or any part of the Products at any time if required by applicable law, effective immediately, which may result in the forfeiture and destruction of all information within Customer's subdomain for any SaaS products.

**7.5. Termination for Convenience**. Customer may terminate the Agreement for its sole convenience in accordance with FAR 52.212-4(l) or similar law or regulation if the clause is applicable to the relevant Order Form.

**7.6. Effect of Termination.** Upon any termination or expiration of this Agreement, Customer and its Authorized Users' right to access and use the Qlik Products and Services shall automatically cease. No refunds or credits of any prepaid fees shall be granted in the event of any termination or expiration. All provisions of this Agreement which by their nature should survive termination shall survive termination, including, without limitation, ownership provisions, warranty disclaimers, indemnity and limitations of liability. Termination of this Agreement or any licenses or subscriptions shall not prevent either Party from pursuing all available legal remedies, nor shall such termination relieve Customer's obligation to pay all fees that are owed.

7.8. Qlik may, without limiting its other rights and remedies, suspend Customer's access to Qlik Cloud at any time if: (i) required by applicable law, (ii) Customer or any Authorized User is in violation of the terms of this Agreement, the Qlik Acceptable Use Policy, or (iii) Customer's use disrupts the integrity or operation of Qlik Cloud or interferes with the use by others. Qlik will use reasonable efforts to notify Customer prior to any suspension, unless prohibited by applicable law or court order.

## 8. General Provisions

**8.1. Recordkeeping, Verification and Audit**. While this Agreement is in effect and for one (1) year after the effective date of its termination, upon request by Qlik but not more than once per calendar year, Customer shall conduct a self-audit of its use of the Qlik Products and, within ten (10) business days after receipt of such request, submit a written statement to Qlik verifying that it is in compliance with the terms and conditions of this Agreement. Qlik shall have the right, on its own or through its designated agent or third-party accounting firm, to conduct an audit of Customer's use and deployment of the Qlik Products and monitor use of Qlik Cloud, in order to verify compliance with this Agreement. Qlik's written request for audit will be submitted to Customer at least fifteen (15) days prior to the specified audit date, and such audit shall be conducted during regular business hours and with the goal of minimizing the disruption to Customer's business.

**8.2. Third-Party Materials.** Qlik Products may incorporate or otherwise access certain open source or other third-party software, data, services, or other materials for the hosting and delivery of the Qlik Products, which are identified in the Documentation (the "Third-Party Materials"). Qlik represents that if the Qlik Products are used in accordance with this Agreement, such use shall not violate any license terms for the Third-Party Materials. Qlik makes no other representation, warranty, or other commitment regarding the Third-

Party Materials, and hereby disclaims any and all liability relating to Customer's use thereof.

**8.3. Connectivity to Third-Party Applications.** Use of Qlik Products to connect or interoperate with or access third-party applications or services may be governed by terms and conditions established by such third party. Third-party application programming interfaces and other third-party applications or services ("Third-Party Applications") are not managed by Qlik, and Qlik shall have no liability for connectivity if any Third-Party Applications are changed or discontinued by the respective third parties. Qlik does not support, license, control, endorse or otherwise make any representations or warranties regarding any Third-Party Applications. Use of Qlik published APIs are subject to the Qlik API Policy located at www.qlik.dev.

**8.4. Commercial Terms.** Qlik Products are a commercial items and commercial off the shelf products as defined in FAR Part 202-1. These Terms reflect (a) standard commercial practices for the acquisition of Qlik Products and (b) terms and conditions that Qlik customarily provides to its other customers. These Terms apply to the Customer's use of Qlik Products as consistent with applicable law and regulation. If the Agreement conflicts with applicable law and regulation (such as FAR Part 12.212(a)), those terms are deleted and unenforceable as applied to any Order Forms. Qlik developed the Qlik Products solely at private expense. All other use is prohibited.

**8.5. Evaluation.** If Customer is provided Qlik Products for evaluation purposes ("Evaluation Products"), use of the Evaluation Products is only authorized in a non-production environment and for the period limited by the corresponding license key or credentials. If Customer is provided access to an evaluation of Qlik Cloud, Qlik will make the applicable Qlik Cloud offering available to Customer for its internal business operations on an evaluation basis free of charge until the earlier of: (a) the end of the evaluation period; (b) the start date of any purchased Qlik Cloud subscription ordered by Customer; or (c) termination by Qlik in its sole discretion. ANY CONTENT IN QLIK CLOUD, AND ANY CONFIGURATION CHANGES MADE TO THE QLIK CLOUD BY OR FOR CUSTOMER, DURING AN EVALUATION MAY BE PERMANENTLY LOST UNLESS: (A) CUSTOMER PURCHASES A SUBSCRIPTION FOR QLIK CLOUD OR (B) CUSTOMER EXPORTS SUCH CONTENT BEFORE THE END OF THE EVALUATION PERIOD. Notwithstanding any other provision in this Agreement, the right to use the Evaluation Products is provided "AS IS" without indemnification, Support, service level credits, or warranty of any kind, expressed or implied. In no event will Qlik's maximum cumulative liability for Evaluation Products exceed one thousand U.S. dollars ($1,000).

**8.6. Early Release Products**. Qlik may, in its discretion, periodically provide certain Customers with an opportunity to test early release features or functionality in connection with Qlik Products. Customer may decline to participate in the testing of such additional features or functionality at any time. Customer acknowledges that such features or functionality are not considered part of the Qlik Products under this Agreement, are not supported, are provided "as is" with no warranties of any kind and may be subject to additional terms. Qlik reserves the right at any time, in its sole discretion, to discontinue provision of, or to modify, any such features or functionality provided for testing purposes.

**8.7. Assignment**. Unless law or regulation prohibit restrictions on transfer, Customer may only assign the Terms, any Order Form, or any right or obligation under the Agreement, or delegate any performance, with Qlik's prior written consent, which will not be unreasonably withheld. Qlik may assign its right to receive payment in accordance with the Assignment of Claims Act (31 U.S.C. § 3727) and FAR 52.212-4(b), and may assign the Agreement if the Anti-Assignment Act (41 U.S.C. § 15) does not prohibit the transfer. Subject to FAR 42.12 (Novation and Change-of-Name Agreements), Customer must recognize Qlik's successor in interest following a transfer of all or substantially all of Qlik's assets or a change in Qlik's name. Any assignment contrary to this Section will be void. The Agreement will be binding upon and benefit the parties and their respective successors and assigns. No agency, partnership, joint venture, fiduciary, or employment relationship is created as a result of this Agreement and neither party has any authority of any kind to bind the other in any respect.

**8.8. Privacy.** Qlik's privacy notices and further information regarding Qlik's privacy measures, including Qlik's Product Privacy Notice, may be found at www.qlik.com.

**8.9. Governing Law and Jurisdiction**. This Agreement is governed by the Federal law of the United Statesy, but excluding any conflict of law rules or the United Nations Convention on Contracts for the International Sale of Goods, the application of which is hereby expressly excluded.. TO THE EXTENT AVAILABLE UNDER APPLICABLE LAW, CUSTOMER EXPRESSLY WAIVES ANY RIGHT TO A JURY TRIAL REGARDING DISPUTES RELATED TO THIS AGREEMENT.

TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, CUSTOMER EXPRESSLY WAIVES ANY RIGHT TO A JURY TRIAL REGARDING DISPUTES RELATED TO THIS AGREEMENT.

**8.10. Force Majeure**. FAR 52.212-4(f) governs all excusable delays defined as an occurrence beyond the reasonable control of the Qlik and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. Qlik will notify the Customer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Customer of the cessation of such occurrence.

**8.11. Trade Restrictions**. Qlik Products and Services are provided subject to the laws and regulations of the United States and other countries on trade restrictions that may prohibit or restrict access by certain persons or from certain countries or territories, including but not limited to sanctions, embargoes and export restraints.

**8.12. U.S. Government End Users**. The Software and Documentation provided in Qlik Products are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Qlik Products and Documentation by the U.S. Government shall be governed solely by the terms and conditions of this Agreement.

**8.13. Notices**. All notices by Customer to Qlik must be in writing and delivered to Qlik: (a) by certified or registered mail or by an internationally recognized express courier addressed to Qlik at 211 S. Gulph Rd., Suite 500, King of Prussia, PA 19406 USA, Attention: Legal Department, or (b) by email to CustomerNotices@qlik.com. Unless otherwise specified in writing by Customer, all notices to Customer shall be sent to the address or email provided to Qlik.

**8.14. Relationship between the Parties**. The Parties are independent contractors. Nothing in this Agreement will be construed to create an agency, joint venture, partnership, fiduciary relationship, joint venture or similar relationship between the Parties.

**8.15. No Waiver**. No term of this Agreement will be deemed waived and no breach excused unless such waiver or excuse shall be in writing and signed by the Party issuing the same. Neither this Agreement nor any Order Form shall be dependent on Customer issuing a purchase order. Customer acknowledges that any purchase order is for its administrative convenience only and that Qlik has the right to issue an invoice and collect payment without a corresponding purchase order. Any additional or conflicting terms or conditions in any purchase order shall have no legal force or effect.

**8.16. Limitation**. Subject to applicable law, no action, regardless of form, arising out of this Agreement may be brought by Customer more than two (2) years after the cause of action arose.

**8.17. Entire Agreement; Severability; Language**. This Agreement, any attachments hereto or documents referenced in the Agreement are the complete statement of the mutual understanding of the Parties and supersedes and cancels all previous written and oral agreements and communications pertaining to the subject matter of this Agreement. This Agreement may not be modified except in writing and signed by both Parties. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid or unenforceable, that provision will be limited to the minimum extent necessary so that this Agreement will otherwise remain in force and effect. In the event of any conflicts or inconsistencies, the Agreement shall take precedence over the Order Form, but only with respect to the specific subject matter of each. For the avoidance of doubt, where an Order Form includes additional and more specific terms and conditions with respect to a concept addressed generally in this Agreement or does not address a concept addressed herein, no conflict shall be deemed to exist. The English language version of this Agreement shall be the governing version used when interpreting or construing this Agreement.

**8.18. Construction.** For purposes of this Agreement: (i) the words “include,” "includes" and "including" are deemed to be followed by the words "without limitation"; (ii) the word "or" is not exclusive; and (iii) words denoting the singular have a comparable meaning when used in the plural, and vice-versa. A Party’s role in drafting this Agreement shall not be a basis for construing this Agreement in any manner against such Party. Any Qlik Order Form and the schedules and exhibits attached thereto are an integral part of this Agreement to the same extent as if they were set forth verbatim herein.

**8.19. Publicity**. Customer hereby grants Qlik the right to list Customer as a customer of Qlik along with other customers in marketing materials such as the Qlik website, customer-facing presentations and press releases to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

## II. QLIK SOFTWARE TERMS

The terms in this Section II apply exclusively to Software licensed by Customer under this Agreement.

### 9. Warranties

**9.1. Software Warranty**. Qlik warrants that the Software will, for a period of ninety (90) days from its Delivery Date (“Warranty Period”), operate substantially in conformity with the applicable Documentation. Customer must assert any claim for breach of this warranty within the Warranty Period. Customer’s exclusive remedy and Qlik’s sole liability with regard to any breach of this warranty will be, at Qlik's option and expense, to either: (i) repair or replace the non-conforming Software; or (ii) if the Software was obtained by purchase, refund to Customer the fees paid by Customer for the non-conforming Software. If Qlik elects to refund the applicable fee paid for the non-conforming Software, then: (i) Customer shall promptly return or demonstrate to Qlik’s reasonable satisfaction that it has destroyed the nonconforming Software and any other related materials provided by Qlik; and (ii) the right to access or use such non-conforming Software will automatically terminate.

**9.2. Exclusions**. Qlik will have no liability for any warranty claim, or any obligation to correct any defect or problem with the Software, to the extent that it arises out of: (i) any use of the Software not in accordance with the Documentation; (ii) any unauthorized modification or alteration of the Software; or (iii) any use of the Software in combination with any third-party software or hardware not specified in the Documentation.

## III. QLIK CLOUD TERMS

The terms in this Section III apply exclusively to the access and use of Qlik Cloud by Customer.

### 10. Customer Responsibilities

**10.1. Content**. Customer acknowledges and agrees that it has sole responsibility: (i) to administer user access to Qlik Cloud and the Content, (ii) for the input and administration of Content in Qlik Cloud, including deletion of Content prior to expiration or termination, (iii) to ensure Qlik has all rights necessary to host, store, adapt or integrate such Content as required to provide Qlik Cloud, and (iv) for maintaining Content on the systems from which they are sourced and making backup copies of Content. Customer hereby represents and warrants on behalf of itself and its Authorized Users that it has all of the rights in the Content necessary for the use, display, publishing, sharing and distribution of the Content and that such use of the Content under this Agreement does not violate any third-party rights, legal obligations, laws, or this Agreement.

**10.2. Authorized Access**. If Customer chooses to have an Authorized User access Qlik Cloud on its behalf, Customer acknowledges that Customer, and not Qlik, is solely responsible and liable for (i) the acts and omissions of such Authorized User in connection with Qlik Cloud; (ii) any Content that Customer requests or instructs the Authorized User to include in Qlik Cloud; and (iii) the issuance, removal and/or deactivation of the credentials issued for such Authorized User.

### 11. Data Security and Privacy

**11.1 Data Security**. Qlik will use commercially reasonable, industry standard security measures in providing Qlik Cloud and will comply with such data security regulations applicable to Qlik Cloud. Qlik has implemented appropriate technical and procedural safeguards to protect and secure Content in accordance with the Information Security Addendum available at www.qlik.com/product-terms. Qlik Cloud offerings are hosted and delivered from a data center operated by a third party provider, which is solely responsible for the underlying infrastructure and hosting of Qlik Cloud. Customer is solely responsible for any breach or loss resulting from: (i) Customer’s failure to control user access; (ii) failure to secure Content which Customer transmits to and from Qlik Cloud; and (iii) failure to implement appropriate and timely backups, reasonable and appropriate security standards and measures, including encryption technology, to protect against unauthorized access.

**11.2. Data Privacy.** The terms of the Data Processing Addendum at www.qlik.com/license-terms (“DPA”) are attached hereto and incorporated by reference when executed by Customer as set forth in the DPA and received by Qlik, and shall apply to the extent Content includes “Customer Personal Data” as defined in the DPA. Customer and Authorized Users are not permitted to upload or store within Qlik Cloud: (i) payment card information subject to Payment Card Industry Data Security Standards (PCI DSS), or (ii) U.S.

Protected Health Information ("PHI") as defined under the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) unless Customer: (a) has executed a Business Associate Agreement for Qlik Cloud ("BAA") with Qlik; and (b) utilizes customer managed key functionality within Qlik Cloud for so long as Customer stores PHI within Qlik Cloud.

## 12. Qlik Cloud Warranty

**12.1. Warranty**. Qlik warrants that Qlik Cloud will perform substantially in accordance with the applicable Documentation when used as authorized under this Agreement. This warranty will not apply: (i) unless Customer notifies Qlik of a claim under this warranty within 30 days of the date on which the condition giving rise to the claim first appears, or (ii) the event giving rise to the warranty claim was caused by misuse, unauthorized modifications, or third-party hardware, software or services. Customer's exclusive remedy and Qlik's sole liability with regard to any breach of this warranty will be, at Qlik's option and expense, to either: (i) repair or replace the non-conforming Qlik Cloud or (ii) terminate the affected Qlik Cloud and refund Customer, on a pro rata basis, any unused, prepaid fees as of the termination effective date, but in no event less than one thousand U.S. dollars (USD $1,000).

**12.2. Warranty Disclaimer**. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, QLIK CLOUD IS PROVIDED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES IMPLIED BY ANY COURSE OF PERFORMANCE OR USAGE OF TRADE, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. QLIK AND ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, PARTNERS, SERVICE PROVIDERS AND LICENSORS DO NOT WARRANT THAT: (I) QLIK CLOUD WILL BE UNINTERRUPTED OR ERROR FREE, (II) QLIK CLOUD IS FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS; OR (III) THE RESULTS OF USING QLIK CLOUD WILL MEET CUSTOMER'S OR AUTHORIZED USERS' REQUIREMENTS. FURTHER, ANY PREDICTIVE SERVICES INCLUDED IN QLIK CLOUD ARE BASED ON CUSTOMER'S CONTENT AND INPUT INTO QLIK CLOUD AND SUCH SERVICES ARE NOT A GUARANTEE OF RESULTS OR FUTURE PERFORMANCE.

## 13. Suspension of Service

Qlik may, without limiting its other rights and remedies, suspend Customer's access to Qlik Cloud at any time if: (i) required by applicable law, including Export Control Laws, (ii)reserved, or (iii) Customer's use disrupts the integrity or operation of Qlik Cloud or interferes with the use by others. Qlik will use reasonable efforts to notify Customer prior to any suspension, unless prohibited by applicable law or court order.

# Support Policy

This Support Policy ("Policy") describes the current practices of Qlik with regard to its provision of Support Services and Maintenance Services for Software as defined below (collectively "Support") to customers with an Agreement ("Customer(s)"). Prior versions of this Policy were titled "Qlik Maintenance Policy" and any reference to such Maintenance Policy in any customer agreement shall be deemed a reference to this Policy. Support services for Qlik Cloud Offerings are located in the Qlik Service Level Agreement.

## 1. Definitions

**"Affiliate"** means any entity which controls, is controlled by, or is under common control with Customer where "control" means the legal, beneficial, or equitable ownership of at least a majority of the aggregate of all voting equity interests of such entity, but only for so long as such control exists

"**Agreement**" means the written agreement for Software between Qlik and Customer, which includes the provision of Support.

**"Authorized Affiliate"** means any Affiliate of Customer that is designated by Customer as authorized to use the Software if permitted under the terms of an Agreement.

**"Documentation"** means the then-current user documentation for the Software, including the product metrics available at www.qlik.com/product-terms, as may be modified by Qlik from time to time.

**"Error"** means any verifiable and reproducible failure of Software to materially conform to the Documentation.

**"Initial Response Time"** means the period commencing when an Error is first reported by Customer's Technical Contact(s) in the manner required by this Policy and ending when a member of the Qlik technical support team logs the report as a Support Case and responds to the Technical Contact(s) by telephone, email, Live Chat or through the Support Portal.

"**Live Chat**" is Qlik's online chat feature that enables Customers to directly message and communicate with Qlik's representatives.

**"Maintenance Services"** means the release of Updates to the applicable Software, which Qlik elects to make generally available to Customers.

**"Product Line**" means a group of related products or items, which have common features, functions, or branding, and are deployed in a common environment. For example, Qlik Sense Enterprise Client-Managed Professional User and Analyzer User are part of the same Qlik Sense Enterprise product line. Qlik Sense Enterprise Client-Managed and Qlik Cloud Offerings are deployed in different environments and are not part of the same Product Line.

**"Qlik Cloud Offering"** refers to any SaaS offering deployed on Qlik's cloud.

**"Release Management Policy"** means the then-current release management policy for the applicable Software as currently set forth at http://www.qlik.com/product-terms, and as may be modified by Qlik from time to time.

"**Self-Service Tools**" means the Knowledge Base (Qlik's online database of content and FAQs about the use and support of the Software), white papers, Community Forums, webcasts, and other materials available in the Support Portal to Customers that are current on Support.

**"Severity 1 Error"** means that the Software is inoperable or not accessible in a production environment due to (i) a server-side failure, but not as a result of scheduled maintenance and/or upgrades, or (ii) any event beyond the reasonable control of Qlik, including but not limited to any interruption of power, telecommunications or Internet connectivity, and any failure of Customer's internal telecommunications equipment, browser or network configurations, hardware and/or third party software.

**"Severity 2 Error"** means that major functionality is materially impacted and not working in accordance with the technical specifications in the Documentation or significant performance degradation is experienced so that critical business operations cannot be performed.

**"Severity 3 Error"** means any Error that is not a Severity 1 Error or Severity 2 Error.

**"Software"** means the generally available release of Qlik's proprietary software in object code form, any Qlik-maintained virtual appliance, and the software API, licensed to Customer under an Agreement. Software excludes early release, technical preview, beta, free trial, or evaluation versions as well as any extensions, objects, open-source projects or code made available without charge on https://qlik.dev/ or other developer forums, and any Software which excludes Support in the terms of use. Software does not include a Qlik Cloud Offering.

“**Standard Business Hours**” means from 08:00 to 17:00 (8:00 am to 5:00 pm), Monday to Friday (excluding national and bank holidays) for the Support Center in the specific geographic region to which the applicable licenses are assigned in Qlik’s records, unless otherwise updated for a Technical Contact in Qlik’s records..

"**Support Case**” means a documented request for Support Services that is registered with Qlik Support in accordance with this Policy and assigned a case number.

“**Support Portal**” means Qlik’s online support website available at https://community.qlik.com/t5/Support/ct-p/qlikSupport.

**“Support Services”** means the technical end-user support for the Software as described in this Policy. Support Services do not include services performed onsite at any Customer facility, consulting or education services, Maintenance Services, or any services not expressly stated in this Policy.

**“Technical Contact(s)”** means Customer’s personnel that have been identified in writing by Customer as the technical contact(s) for Customer and authorized to contact Qlik for support.

**“Update”** means any Software enhancement, modification or Error correction made available in accordance with the Release Management Policy, which Qlik elects to make generally available to its customers as part of Maintenance Services. Updates do not include new or separate products which Qlik offers only for an additional fee to its customers generally.

## 2. Overview

2.1 Qlik will provide Customer with Support Services and Maintenance Services for the Software in accordance with this Policy and the level of coverage purchased by Customer (if applicable) as well as any applicable terms in the Agreement, subject to Customer’s timely payment of the applicable Support fees or subscription fees.

2.2 In order to receive Support Services, Customers experiencing an Error with the Software shall enter the Support Portal and select the Live Chat feature to input a description of the Error. Qlik Support will either respond to the chat directly or open a Support Case for Customer. If the issue is resolved via the chat, a Support Case will not be established. A Support Case may be established by Qlik for any Error, and also may be created by Customer for a Severity 1 Error only within the Live Chat feature.

2.3 Unless otherwise expressly set forth herein, all references in this Policy to response times or communications from Qlik shall only apply during Qlik’s Standard Business Hours, regardless of when a support matter is reported to Qlik. By way of example, Standard Business Hours for licenses assigned to New York in Qlik’s records would be 08:00 to 17:00, Eastern Time, Monday to Friday (excluding U.S. federal and bank holidays). Times expressed as a number of “business days” include Standard Business Hours.

2.3 Any Support Services provided by Qlik hereunder will be provided in the English language or, as applicable, such other languages that may be specified on the Support Portal, which may change from time to time. The availability of Support provided in any language other than English is provided at Qlik’s sole discretion and is not guaranteed by Qlik and will depend on the location of Qlik’s technical support personnel providing such support, including whether or not Customer is entitled to contact that particular support line based on the type of Support Services purchased and Customer’s geographic location.

## 3. Support Levels for Support Cases

3.1 Enterprise Support Coverage for Software.

3.1.1 Scope of Coverage. Customers with Enterprise Support receive support for Support Case Error determination, verification and resolution (or instruction as to work-around, as applicable) twenty-four (24) hours a day, seven (7) days a week, 365 days a year for Severity 1 Errors and during Qlik’s Standard Business Hours for Severity 2 and Severity 3 Errors.

3.1.2 Support Case Handling. Qlik will assist Enterprise Support Customers in issue analysis to determine whether or not the technical issue is related to the third-party hardware or software. In order to isolate the issue, Qlik reserves the right to request that the third-party hardware or software be removed. Qlik may in its discretion reach out to third-party vendors based on the established Technical Support Alliance Network (TSANet) to troubleshoot the issue. TSANet is a vendor-neutral global support alliance where companies work together to support mutual customers more effectively. Qlik will only engage TSANet for Customers who are using supported configurations.

3.1.3 Update Information. Customers may contact Live Chat or Qlik Support for information regarding Updates performed by Customer, such as installation instructions, release documentation, and general guidance for multiple environments.

3.1.4 Qlik will use commercially reasonable efforts to respond to a Support Case (a) within the initial response time targets set forth in the table below for Severity 1 Errors reported by a Technical Contact to Qlik via the Support Portal or (b) within the Initial Response Times set forth in the table below for Severity 2 and Severity 3 Errors that are reported by a Technical Contact to Qlik via the Support

Portal. Qlik will respond to Customer's Technical Contact via the Support Portal, or at Qlik's discretion, via telephone or teleconference. Severity 2 & 3 Errors will be initially logged and acknowledged by Qlik during Qlik's Standard Business Hours in the region where the Error is reported. Provided that Customer provides Technical Contacts in other regions that are available to help troubleshoot issues, all Severity 1 Errors will be addressed and handed over between regions for as long as the Customer provides the available Technical Contacts in such region(s). Qlik shall use commercially reasonable efforts, consistent with industry practice, to investigate such Support Cases to determine whether there is an Error present. If Qlik determines that an Error is present, Qlik will use commercially reasonable efforts to correct the Error and/or provide a workaround, including, without limitation, by providing Customer with an Update. Qlik will communicate with Customer with at least the frequency targets set forth in the table below until the Error is resolved (in accordance with Section 4 below) or a work-around is provided.

**Enterprise Support Coverage for Support Cases**

| Severity Level | Initial Response Time | Communication Frequency |
|---|---|---|
| Severity 1 Error | 30 minutes, 24x7** | Every 4 hours, 24x7** |
| Severity 2 Error | 1 hour* | 48 Hours* |
| Severity 3 Error | 4 hours* | Weekly* |

*During Standard Business Hours
**For Software that has been announced as End of Life, Standard Business Hours apply to Response Times and Communication Frequency

## 4. Error Resolution and Escalation for Support Cases

4.1 An Error is considered to be resolved upon the earlier to occur of the following: (i) Qlik and Customer mutually agree in writing that the issue or problem is resolved; (ii) Qlik has provided Customer with an Update; (iii) a technical workaround solution is provided and is reasonable in Qlik's discretion; (iv) Customer requests that Qlik close the Support Case; or (v) the Support Case has been left open by the Customer for ten (10) consecutive business days, during which period Qlik has not received a response from any of Customer's Technical Contacts.

4.2 Exclusions. Notwithstanding anything in this Policy to the contrary, Qlik will have no obligation to provide any Support Services in connection with: (i) any issue or problem that Qlik determines is not due to any Error or deficiency in the Software (including without limitation, issues or problems caused by stand-alone third party software products or services used in conjunction with the Software, the Internet or other communications, Customer network or browser matters, or login issues); (ii) use of the Software other than in accordance with the Documentation and the Agreement; (iii) any issue or problem that is not included in a Support Case; (iv) use of the Software provided on a trial or evaluation basis or for which Customer has not paid any fees; (v) any Errors or problems with the applicable Software that are not reproducible; (vi) any Error or problem that is reported by Customer via any Qlik support telephone number or email address; or (vii) any Errors or problems with the Software that result from: (a) the use of the Software with software or hardware not designed for use with the operating systems approved by Qlik in the Documentation; (b) the use of the Software with hardware that does not satisfy the minimum system requirements specified by Qlik in the Documentation; (c) changes, modifications, or alterations to the Software not approved in writing by Qlik or its authorized representatives (d) use of the Software with third party operating systems, databases, data sources, network software and client applications that are no longer supported by the related product vendors, or (e) use of other than a Supported Version of the Software as defined in the applicable Release Management Policy. If Qlik does correct any of the Errors described in subsections (a)-(e) above, or otherwise provides support for Software that is not covered by the terms and conditions contained in this Policy, such Error resolution or support will be provided only following Customer's written request and approval of all charges, and Customer will be invoiced for such support at Qlik's then-current "time and materials" rates for such services. Without limiting any of the foregoing, Qlik has no obligation to provide support for any third-party software, data, or other materials distributed or bundled with a Software.

## 5. Updates

In addition to its obligations under Sections 2 and 3 of this Policy, Qlik will make Updates available to all Customers with a current Agreement, when and if Qlik elects to make them generally commercially available. All Updates provided to any Customer under this Policy will be made available at Qlik's discretion, in a form of digital medium or via the Qlik Software download site. Unless otherwise agreed in writing by Qlik, Customer shall be responsible for installation of all Updates. Qlik is under no obligation to develop any future functionality, programs, services, or enhancements.

## 6. Customer's Obligations

6.1 Customer will provide timely information and access to knowledgeable resources as reasonably required to provide Support. Qlik's support obligations shall be excused to the extent Customer fails to cooperate in this regard.

6.2 The Customer shall: (i) not request, permit or authorize anyone other than Qlik (or a Qlik-authorized partner or provider) to provide any form of Support Services in respect of the Software; (ii) cooperate fully with Qlik's personnel in the diagnosis or investigation of any Error or other issue or problem with the Software; (iii) be responsible for purchasing, installing and maintaining all hardware and operating systems required to use and support the Software; (iv) be responsible for maintaining all third party software not explicitly licensed under the Agreement; and (v) be fully responsible for the actions of any third party (including any Qlik-authorized partner or provider) that it allows to access any information relating to Support Services.

6.3 Customer's contact with Qlik in connection with Customer's requests for support and reports of Errors shall be solely through its Technical Contact(s). The Technical Contact(s) shall: (i) serve as the internal contact(s) for Customer's and its Authorized Affiliates' personnel who are authorized to use the Software per the terms of the Agreement; (ii) be responsible for initiating all requests by, and maintaining all records of, the Customer and its Authorized Affiliates relating to Support Services; (iii) serve as the contact(s) with Qlik on all matters relating to Support Services; and (iv) be responsible for providing information and support, as requested by Qlik, to assist in the reproduction, diagnosis, analysis, and resolution of Errors. The maximum number of Technical Contacts for each Customer is six (6), regardless of the number or types or quantities of licenses or subscriptions purchased for the Software. Customer shall ensure that its Technical Contacts comply with any reasonable training requirements for the Technical Contact(s) upon notification by Qlik. Subject to the previous sentence, Customer may change its Technical Contact(s) by notifying Qlik in writing.

6.4 If Qlik is unable to reproduce a problem or the solution requires modifying Software configuration parameters, Qlik may require Customer to provide remote access in order to continue providing support. Customer shall ensure that a functioning system enabling Qlik to have remote access to Customer's technical equipment is installed (subject to Customer's reasonable security measures and policies) and that satisfactory communication between the parties' computer systems is possible. Customer agrees to be solely responsible for protecting and backing up its equipment, software, and data prior to any such access. Qlik accepts no liability in connection with remote access support. A request for a remote connection will come only after other options are explored.

6.5 Customer will be responsible for primary support of any Authorized Affiliates in connection with their use of the Software in accordance with the terms of the Agreement. Customer is solely responsible for: (i) distributing all Updates to its Authorized Affiliates (where applicable); (ii) passing on to its Authorized Affiliates all support materials as appropriate; and (iii) providing software support, including operational instruction, problem reporting and technical advice to its Authorized Affiliates, in each case of (i), (ii) and (iii) above, as necessary to enable the Authorized Affiliate to continue to use the Software as authorized under the Agreement. Customer's Authorized Affiliates, as well as its contractors and third-party users, may not contact Qlik directly for support of the Software unless designated as a Technical Contact by the Customer.

6.6 Qlik supports the Software in designated operating systems as described in the Documentation and not specific hardware configurations. If Customer is running the Software on a virtual environment, Customer and the virtual environment vendor will be responsible for any interactions or issues that arise at the hardware or operating system layer as a result of the use of a virtual environment. Qlik reserves the right to request Customers to diagnose certain issues in a native designated operating system environment, operating without the virtual environment, as needed to determine whether the virtual environment is a contributing factor to the issue.

6.7 Customer is expected to use a non-production environment for development and to conduct sufficient testing before making any updates to production.

6.8 For certain services provided under this Policy, the transmission of machine logs and/or sharing of data via screen share may be required. For avoidance of doubt, Customer shall not include any business sensitive and/or personal information via transmissions relating to Support Services. Accordingly, Qlik shall not be deemed a Data Processor under EU General Data Protection Regulation (as amended) in providing support for the Software. Customer shall take reasonable measures to anonymize such data before providing the data to Qlik. However, should Qlik agree to accept any log files or other information containing personal data, Qlik will comply with Qlik's privacy policies,attached hereto and available to view online at www.qlik.com.

## 7. Additional Terms

7.1 Support is included in the subscription fee for all subscriptions and provided by Qlik. Customer is required to separately purchase Support on all perpetually licensed Software for a twelve (12) month period beginning on the delivery date of the Software (the "Initial Support Period"). In addition, Customer must maintain support across (i) all perpetual licenses within the same Product Line and (ii) all licenses, whether perpetual or subscription, within the same deployment. Customer must be current on Support for all previously purchased licenses in the same Product Line in order to purchase additional licenses.  In the event the Customer elects not to renew an Agreement for its perpetual licenses, the non-renewal must apply to all licenses within the same Product Line.  Notwithstanding the foregoing, any Software or subscriptions purchased as a bundle, package, or special promotion (e.g., enterprise licenses) must be supported together at a uniform level, regardless of whether such Software purchase includes multiple Product Lines.

7.2   Unless otherwise agreed in writing, Agreements for perpetually licensed Software maybe renewed for successive twelve (12) month periods (each, a "Support Period")by executing a written order. Support fees for any additional Software purchases will be prorated to achieve a common annual Support Period with existing licenses, but does not relieve Customer of its payment obligations for the remainder of the Support Period.  For avoidance of doubt, Customer is responsible to pay the entire Support fee for the Initial Support Period on all additional purchases of Software regardless of any proration of Support fees.

7.3   Reinstatement of lapsed or cancelled Agreements for perpetually licensed Software will be subject to payment by Customer of (a) the then-current annual Support fees payable for the 12-month period beginning on the date of reinstatement and (b) the aggregate Support fees that would have been payable for the relevant Software during the period of lapse in the absence of termination or non-renewal, provided that (i) the combined reinstatement fees are paid within twelve (12) months after the date of the lapse and (ii) Customer pays Qlik a Support reinstatement fee equal to twenty-five percent (25%) of the total Support fees payable to Qlik for all applicable Software licensed by Customer.  Reinstatement beyond this date will be at Qlik's sole discretion.  Reinstatement fees may be assessed once notice of cancellation or non-renewal is provided, even if a request for reinstatement is provided prior to the expiration of the current Support Period.

7.4   Open Source.  Qlik may open-source certain libraries available for use with Software as described in the Documentation ("Qlik Libraries") at https://qlik.dev/support. Qlik Libraries are eligible for support, provided that Qlik shall only be obligated to support: (i) the most current release, (ii) Qlik Libraries which have not been changed, modified or altered in any manner except by Qlik, and (iii) Qlik Libraries used in accordance with the Documentation. Please review https://qlik.dev/support for more information. Any other open-source software leveraging and extending a Software (an "Extension") and released by Qlik on various online communities is supported solely by the open-source community.  Extensions, which are developed by Qlik's partners, including certified Extensions, are also not eligible for support under this Policy.

7.5   Qlik may elect to make certain software available free of charge for trial, evaluation, or other purposes ("Freeware").  Support for Freeware, if any, will be provided at Qlik's discretion and in accordance with the license terms for such Freeware.

7.6   Support fees are payable annually . Where Customer receives support services from an authorized reseller, such support services will be provided pursuant to a separate written agreement between Customer and the authorized reseller.

## 8. Changes to Policy

Subject to the terms of the Agreement, Qlik reserves the right, at its discretion, to non-materially change the Policy at any time based on prevailing market practices and the evolution of Qlik's products and services.

## 9. Disclaimer

THIS POLICY DEFINES A SERVICE ARRANGEMENT AND NOT A WARRANTY.  THE SOFTWARE IS SUBJECT EXCLUSIVELY TO THE WARRANTIES SET FORTH IN THE APPLICABLE AGREEMENT.  THIS POLICY DOES NOT CHANGE OR SUPERSEDE ANY TERM OF ANY SUCH AGREEMENT. TO THE EXTENT THERE IS A CONFLICT BETWEEN A TRANSLATED VERSION OF THIS POLICY AND THIS ENGLISH VERSION, THE ENGLISH LANGUAGE VERSION WILL PREVAIL.

# Qlik® Consulting Services Product Terms

These Consulting Services Product Terms ("Consulting Product Terms") provide a description of Qlik services provided with the Consulting Services product offerings below. These Consulting Services product offerings are governed by these Consulting Product Terms as well as any existing services agreement between Qlik and the Customer which governs the provision of consulting services, or if none, the Consulting and Education Services Terms attached hereto and at www.qlik.com/legal-agreements ("Services Agreement"). In the event of any conflict between the Services Agreement and these Consulting Product Terms, these Consulting Product Terms will prevail.

## A. General Consulting Services

### 1. RESERVED

.

### 2. Signature Success

**2.1** Signature Success is a package of key services, including but not limited to Consulting, governance services, technical account management, Education Services, and Support, which are designed to assist Customer in building a successful foundation for a Qlik deployment(s). The offering focuses on aligning key Services to assist in the delivery of the success goals outlined in the Customer Success Plan (CSP), which is further detailed below. The offering aims to help Customer with:

- Aligning the Qlik platform to Customer's business objectives and strategy
- Driving product adoption and user enablement
- Enabling Service scalability when and where Customer needs it, reducing the complexity of Customer's engagement model with Qlik
- Leveraging the collective strengths of the entire Qlik ecosystem

**2.2** The following organizational roles and Service delivery are part of Signature Success (described in further detail below):

- Customer Success Manager (CSM)
- Customer Success Engineer (CSE)
- 24 x 7 technical support for Severity 1 Errors
- 15 min SLA target for Severity 1 Errors
- Priority escalations management
- 300 Qlik Credits (per year) – for consumption of Consulting and/or Education Services
- Unlimited Corporate License for Qlik Continuous Classroom and Talend Academy
- Regular business reviews

**2.3** Signature Success is offered as a subscription and if applicable, must be co-terminous with a Customer's product Subscription Period.

**2.4 Customer Success Manager (CSM)**

a. Signature Customers will be assigned a CSM. A CSM refers to a Qlik resource who works proactively with Customer as a business advocate and acts as the first point of contact with Qlik. The CSM will be available during local business hours and are typically responsible for managing a select number of key strategic Customer accounts during the term of the contract. The CSM is responsible for working with Customer to create a joint Customer Success Plan (CSP). The CSP will outline the use cases, outcomes, and key business values to be achieved with corresponding success metrics. The CSM will then be responsible for aligning the appropriate resources available to the account to deliver against the CSP's metrics.

b. CSM activities may include the following:

- Create a tailored CSP to document the definition of success for an account and the proposed steps needed to achieve that outcome.
- Facilitate monthly business reviews with Qlik's team of experts to review progress of the CSP and explore how Customer can leverage Qlik solutions to drive innovation.
- Coordinate CSO Services consumption in line with success targets in the CSP
- Assist Customer in designing an end-to-end user journey by facilitating access to our onboarding, collaboration, promotion and continuous learning resources.
- Workshops to Identify personas, pathways for adoption, and necessary enablement. Identify the communication plan and monitoring of adoption for specific personas, as well as counter actions for lower than anticipated adoption.
- Be a first point of contact to engage with other CSO teams to ensure that any issues that might arise are managed through to successful resolution.
- Create workshops on data and analytics maturity. Work with Customer to assess and benchmark Customer's current state, then outlining strategies and tactics to progress the organizations maturity.
- Establish program coordination to identify the various business project/workstream dependencies and highlight those interlocks to the Customer Success Plan. These include:

- ○ Facilitation of Qlik Consulting Services engagement – connecting the Customer and Qlik Consulting, managing the credit certificate process.
- ○ Regular check-ins on Consulting Services progress and outcomes
- ○ Coordinate and assist CSE with activities, e.g. workshops, product demos, roadmap, etc.
- ○ Education and enablement assistance – persona mapping, assist developing learning paths and credits for instructor-led training.

**2.5 Signature CSE.** Signature Success includes access to Tier 3 Signature CSE as per the terms outlined below.

**2.6 Support.** Signature Success includes access to Support Services as per the terms outlined in Section 3.4 below.

**2.7 Qlik Credits.** The CSP will include a plan of the Consulting and Education Services that will be delivered by Qlik in order to meet the objectives outlined in the CSP. . Unused Credits may not be rolled forward into subsequent annual periods (within a multi-year subscription) or into any renewal period of the Signature Services.

a. Use of Credits. Qlik Credits may be used by Customer to purchase consulting services and training solely from the selection of offerings available at www.qlik.com/signatureservicescatalog (the “Qlik Credit Catalog”). Qlik Credits may not be used against engagements not included in the Qlik Credit Catalog and may only be used for Consulting and Education Services in the country of purchase. The Qlik Credit Catalog is subject to change from time to time in Qlik’s reasonable discretion.

b. To redeem Qlik Credits for Services from the Qlik Credit Catalog, the CSM will provide to the customer a Customer Redemption Certificate (CRC) including the name of the specific offering being purchased, the number of credits expected to be consumed, and any travel expenses. Upon submission of the CRC to a Designated Customer Contact, Customer shall have seven (7) days to reject the CRC before Credits are redeemed. For the avoidance of doubt, an SOW shall not be required to consume the Qlik Credits.

c. Additional Credits. Customer may purchase additional Qlik Credits (as defined in the Signature Terms) to use within Customer’s existing Subscription Period.

**2.8 Education Services Entitlements.** Signature Success includes access to Education Services as per the terms in Section 3.6 below.

**2.9 Estimated Expenses.** A preliminary estimate of travel expenses is ten percent (10%) of the total fees paid for Signature Success. Actual expenses may vary. Customer is encouraged, but not required, to include an allowance for this amount its purchase order to Qlik. Expenses will not be incurred without Customer’s prior written consent and will not be invoiced unless incurred.

**2.10 Designated Customer Contact.** Customer may elect to appoint individual(s) who are authorized and responsible for communicating with Qlik regarding Customer’s consumption of the Signature Success benefits (including but not limited to, scheduling matters and/or the redemption of any Qlik Credits) (each such individual, a “Designated Customer Contact”). Designated Customer Contacts may be specified in an Order Form or otherwise in writing from Customer to Qlik. If Customer chooses to appoint a Designated Customer Contact, Customer hereby represents and warrants that each Designated Customer Contact is authorized to make such decisions and act on Customer’s behalf and that Qlik may rely on the written communications of a Designated Customer Contact in its performance hereunder. Customer may change its Designated Customer Contact at any time upon written notice to Qlik.

## 3. Signature CSE

**3.1 Signature CSE.** Signature CSE is a subscription service that includes access to a Qlik resource, who serves as a designated point of contact providing technical advisory services on a given Qlik Product. The Qlik resource may be exchanged up to three (3) times per year during the Subscription Period. Each resource exchange requires advance notice via email to the currently assigned Qlik resource and is subject to the availability of resources with the requisite expertise. Signature CSE typically include the following key activities based on Tier. Activities shall be deemed as completed at Qlik’s discretion.

| CSE Tier* | Tier 3<br>$100k USD to $200k USD | Tier 2<br>$200k USD to $400k USD | Tier 1<br>$400k USD |
|---|---|---|---|
| | Success Plan for technical outcomes | Success Plan for technical outcomes | Success Plan for technical outcomes |
| | Technical Environment assessment | Technical Environment assessment | Technical Environment assessment |
| | Roadmap/New Feature overviews | Roadmap/New Feature overviews | Roadmap/New Feature overviews |
| | Ongoing Advisory/technical Guidance | Ongoing Advisory/technical Guidance | Ongoing Advisory/technical Guidance |
| | Critical Issue technical collaboration | Operational assessment | Operational assessment |
| | Onboarding and CSP Planning | Critical Issue technical collaboration | Critical Issue technical collaboration |
| | | App/DI Pipeline/Data Governance best practice review | Interactive instruction |
| | | Proactive Technical Adoption Insights (Cloud only, subject to telemetry availability) | App/DI Pipeline/Data Governance best practice review |
| | | Onboarding and CSP Planning | Proactive Technical Adoption Insights (Cloud only, subject to telemetry availability) |
| | | | Architecture review and platform roadmap plan |
| | | | Program Governance |
| | | | Onboarding and CSP Planning |
| | | | Business reviews |

*CSE Tier is determined based on Customer's annual subscription fee in USD or local equivalent for the Qlik Products on the Order Form on which Signature CSE is purchased. The Signature CSE Services shall only be provided in connection with the Qlik Products on the Order Form on which Signature CSE is purchased.

Activity definitions are as follows:

| Activity | Description |
|---|---|
| Success Plan for technical outcomes | Plan created and managed with the Customer to align CSE and Customer responsibilities against Customer technical objectives. |
| Technical Environment Assessment | Technical environment assessments will vary based on the Customer. Defined by the CSE and agreed with the Customer via the success planning process, or in response to an emerging issue. May focus on one or more areas depending on the need of the Customer, or advice of the CSE - e.g. infrastructure, platform set up, performance review, app or pipeline assessment etc. Technical environment assessments will typically take no more than one day to complete. |
| Roadmap/New Feature Overviews | CSE led conversation, tailored to Customer based on their use cases and upcoming technical objectives |
| Ongoing Advisory/Technical Guidance | Provide technical and solutions guidance to aid in the execution of the Customers deployment. Typical guidance sessions are no more than 2 hours in duration |
| Operational Assessment | The outcome would be remediation plan/objectives and supporting related advisory/guidance sessions. Examples include:<br>• Review of monitoring/logging/alerting setup.<br>• Review against best practices for operational efficiency (e.g. CI/CD, Automation etc.).<br>• Review of operational processes (e.g. issue triage, capacity mgt, incident/problem mgt).<br>• Ops team skill gap assessment (admin, troubleshooting, working with tech support). |
| App/DI Pipeline best practice reviews | Review of app/DI data pipeline against best practices (incl. for performance optimization). DI pipeline includes Replicate task or Talend Studio job for example. |
| Adoption Insights | Provide advice/enablement on capabilities/features not used based on cloud telemetry. |
| Architecture review and platform roadmap plan | Review of Customer architecture and set up, best practices. Includes remediation recommendations and plan. |
| Interactive Instruction | Detailed interactive instruction or assistance can be provided to Customer teams during working sessions, to help the Customer implement specific, challenging elements of a solution. In certain situations, sample/prototype scripts or configuration can be provided to accelerate project or operational delivery. Typical engagements are no more than 2 hours in duration and consecutive sessions cannot be continuations of the same subject matter. |
| Critical Issue technical Collaboration & Escalation | Typical activities include:<br>• Monitor severity one cases and engage with the Customer and Qlik Support to facilitate communication and updates.<br>• Provide guidance to Customer when struggling to diagnose or isolate issue relating to Qlik platform.<br>• Help accelerate sharing of diagnostic info to Tech Support if Customer is uncertain on how/what to share, ensure Customer understands remediation activities, escalate when needed within Qlik. |
| Program Governance | Overall coordination and alignment of customers business objectives with service delivery |
| Onboarding and CSP Planning | Customer onboarding and Development, maintenance of customers CSP (Customer Support plan) |
| Business reviews | Regular business reviews and assess the progress of the tasks outlined in the CSP |

**3.2** The activities outlined above are available during regional business hours. Delivery resources are typically responsible for managing multiple Customer accounts during the term of the contract.

**3.3** **Supplemental Service.** Signature CSE is intended to supplement and enhance Support Services and are not available on a standalone basis. Signature CSE is offered for a twelve (12) month period, provided however, that Signature CSE shall automatically terminate in the event that Support Services (or subscription) are not renewed by the Customer or are otherwise terminated.

**3.4** **Support.** In addition to any product Support provided to Customer pursuant to the Qlik Support Policy or Service Level Agreement, Customer will be entitled to the additional benefits set forth below. For the avoidance of doubt, the benefits of this section 3.4 require Customer to remain subscribed to Qlik Support for the duration of the Subscription Term.

- Priority Call Access: When contacting Qlik Customer Support, Customer will have access to senior Technical Support Engineers (TSE's) to assist in case resolution. Customer will be prioritized in the call queue over other non-Signature Customers.
- 24 x 7 technical support for Severity 1 Errors: Signature provides the Customer with enhanced availability for all Severity 1 Errors as defined in the Support Policy available here: https://www.qlik.com/us/legal/product-terms.
- 15-minute SLA target for Severity 1 Errors: Qlik will use commercially reasonable efforts to respond within 15-minutes to Severity 1 Errors reported by a Customer Technical Contact to Qlik via telephone.
- Designate up to eighteen (10) technical contacts within Customer's organization to interact with Qlik Support

**3.5** **Qlik Credits**. Signature CSE Customers have the option to purchase Qlik Credits per the terms outlined in section 2.7. Signature CSE subscriptions do not include any Qlik credits as part of the standard subscription.

**3.6** **Education Services Entitlements.** During the Subscription period, Customer will be provided access to one of the below Education Services, depending on Customer's Qlik Product licenses. Please refer to the Education Services Product Terms for additional information.

- Qlik Continuous Classroom Qlik Hosted (QCCQH): Customer will be provided access to all self-paced learning content for an unlimited number of named employees.

- Talend Academy: Customer will be provided access to all self-paced learning content for an unlimited number of named employees.

## B. Consulting Services- Qlik Products

Consulting Services- Qlik Products refers to consulting services provided in connection with the analytics and data integration products identified below.

### 1. Qlik Data Integration Starter Service

**1.1 CDC Data Streaming, Data Lake (DL) or Data Warehouse (DW) Starter Service.** Leveraging Industry best practice Qlik will work with the Customer to provide enablement and implementation expertise and solution deployment for either stand-alone Data Streaming (Replicate) or Data Streaming together with Data Warehouse Automation or Data Lake Creation (Compose) in Customer's environment. In addition, Qlik will work to integrate it with existing Customer systems including environment promotion from non-production to production.

**Prerequisites for CDC Data Streaming & Data Lake/Data Warehouse Starter Services.**
Qlik will perform a remote "pre-assessment" prior to beginning implementation. All prerequisites for the pre-assessment must be met prior to commencing work.

Services include the following:

- Remote Customer environment pre-assessment.
- Qlik Data Integration Blended Learning for up to 2 attendees.
- An architecture review and subsequent development of a best practice design architecture.
- Replicate installation (1 non-production server & 1 production server)
- Enterprise Manager installation.
- Implementation assistance for the LogStream endpoint is limited to 2 targets.
- Replicate configuration:
  - o Up to 3 source endpoints, 2 target endpoint.
  - o Up to 10 transformations limited to timestamps and simple name changes.
  - o Up to 100 tables/2 TB initial load.
  - o Apply and store changes.
  - o Up to 7 tasks.
  - o Does not include SAP on Db2 (LUW, z/OS) and HANA. These sources can be accommodated but will require the purchase of additional consulting assistance due to the complexity of integration.
- Compose configuration (of either):
  - o Compose for Data Lakes configuration (Up to 20 calculations, up to 5 storage tasks, data refreshed).

    **or**
  - o Compose for Data Warehouse configuration (Up to 20 calculations, 1 data mart, 3 fact tables, 5 dimensions, 1 Model, 2 projects).
    - ▪ Limit of 20 tables for the model.
    - ▪ RDBMS Sources only (does not include SAP on Db2 (LUW, z/OS, iSeries) and HANA). These sources can be accommodated but will require the purchase of additional consulting assistance due to the complexity of integration.
    - ▪ Limit scheduler to 2 workflows
    - ▪ No non-Replicate sources.
- Configuration documentation.
- If desired, Qlik will perform a high-level pre-production health-check to help ensure readiness for production deployment.
- Up to 6 months access to a CSE per the terms outlined in section 3.

### 2. Qlik Cloud Starter Services

The Qlik Cloud Starter Services offerings are comprised of a combination of Consulting and Education Services intended to assist Customers who are new to the Qlik Cloud Services (QCS) or Qlik Government Services (QGS) SaaS Platforms

**2.1 Qlik Cloud Starter – New Qlik Customer**
Qlik Cloud Starter is intended for Customers who are not currently active users of Client Managed Qlik Sense or QlikView and may include a combination of Consulting and Education Services. Any Education Services below are subject to the Education Services Terms at www.qlik.com/product-terms.

Services may include the following:

- **Deploy and Administer Qlik Sense SaaS Training** – Blended Training – Attendance by up to two (2) Customer personnel of the Deploy and Administer Qlik Sense SaaS Blended Training Course for 6 months (180 days).
- **Create Visualizations with Qlik Sense Training** – Blended Training – Attendance by up to five (5) Customer personnel of the Create Visualizations with Qlik Sense Blended Training Course for 1 year (365 days).
- **Data Modeling for Qlik Sense Training** – Blended Training - Attendance by up to two (2) Customer personnel of the Data Modeling for Qlik Sense Training Blended Training Course for 1 year (365 days**).**
- **Configuration of Tenant.** Qlik will provide configuration of Customer's Qlik Tenant including user authentication either via the Qlik identity provider or to accept a compatible Customer identity provider without the use of custom coding, configuration of SMTP, and configuration of Customer user authorization for governing Space access. Qlik will also configure standard

Monitoring Applications and standard Demonstration Applications and provide basic enablement to a Customer on the monitoring of their new Qlik environment.

- **Current State Review.** Qlik will work with the Customer personnel to define a target solution design and high-level migration roadmap with the Customer. Qlik will assist with:
  - A baseline inventory of existing BI applications or reports including relevant data sources and business use-cases. Inventory will include applications and reports associated with up to ten (10) business use-cases to be established and mutually agreed at the outset of the engagement.
  - Identify and present opportunities, risks, and recommended mitigations for migration to Qlik Cloud consistent with leading practices.
- **Basic Application Development**. Qlik will work with Customer business users to understand their needs and specific application requirements. Based on this work, Qlik will define a layout and use cases for the application to support and create an application based on these requirements, working with business users to refine the application based on business user feedback. The application will include data from one (1) data source, up to three (3) source tables, up to ten (10) master measures, and up to five (5) million rows. The implementation of row or column level security is not included.
- **Advisory Presentation – Leading Practices -** Qlik will provide a presentation for basic enablement on the following topics:
  - Application Access for End Users.
  - Application Development Lifecycle including Publishing to Production.
  - Onboarding New Users.

**Pre-Requisites**

- Acquisition of licenses for QCS or QGS SaaS platform.
- Customer will provide a named individual(s) for registration to the instructor led training.
- Customer will provide access to relevant resources (IdP administrator, existing BI administrator, business analysts, BI developers, database administrator, data architect, etc.) as needed through the project.
- Customer will configure identity provider, data sources and existing deployments as needed in a timely manner to support implementation.
- Technical prerequisites and source/target setup instructions will be shared following purchase, and the expectation is that those would be completed prior to engagement start.

### 2.2 Qlik Cloud Starter – Current Qlik Sense Customer

Qlik Cloud Starter - Current Qlik Sense Customer is intended for Customers who are currently active users of Client Managed Qlik Sense and may include a combination of Consulting and Education Services. Any Education Services below are subject to the Education Services Terms at www.qlik.com/product-terms.

Services may include the following:

- **Deploy and Administer Qlik Sense SaaS Training** – Blended Training – Attendance by up to three (3) Customer personnel of the public Deploy and Administer Qlik Sense SaaS Blended Training Course for 6 months (180 days).
- **Configuration of Tenant.** Qlik will provide configuration of Customer's Qlik Tenant including user authentication either via the Qlik IdP or to accept a compatible Customer identity provider without the use of custom coding, configuration of SMTP, and configuration of Customer user authorization for governing Space access. Qlik will also configure standard Monitoring Applications and standard Demonstration Applications and provide basic enablement to a user on the monitoring of their new Qlik environment.
- **Current State Review.** Qlik will work with the Customer personnel to define a target solution design and high-level migration roadmap with the Customer. Qlik will assist with:
  - A Baseline inventory and basic analysis of existing Client Managed Qlik Sense applications in one production environment using a Qlik Consulting SaaS readiness utility.
  - Identify and present opportunities, risks, and recommended mitigations for migration to Qlik Cloud consistent with leading practices.
- **Basic Application Development.** Qlik will work with Customer business users to understand their needs and specific application requirements. Based on this work, Qlik will define a layout and use cases for the application to support and create an application based on these requirements, working with business users to refine the application based on business user feedback. The application will include data from one (1) data source, up to three (3) source tables, up to ten (10) master measures, and up to five (5) million rows. The implementation of row or column level security is not included.
- **Advisory Presentation – Leading Practices.** Qlik will provide a presentation for basic enablement on the following topics:
  - Application Access for End Users.
  - Application Development Lifecycle including Publishing to Production.
  - Onboarding New Users.
- **Advisory Presentation – Contextualized Capabilities.** Qlik will provide a presentation in the context of goals shared by the Customer throughout the engagement on the capabilities and practices the Customer may wish to leverage on the QCS platform, and how the Customer might consider leveraging them to meet their objectives.

**Pre-Requisites:**

- Acquisition of licenses for QCS or QGS SaaS platform.
- Customer will provide a named individual for registration to the instructor led training.
- Customer will provide access to relevant resources (IdP administrator, existing BI administrator, business analysts, BI developers, database administrator, data architect, etc.) as needed through the project.
- Customer will configure IdP, data sources and existing Qlik deployments as needed in a timely manner to support implementation.
- Technical prerequisites and source/target setup instructions will be shared at the start of the engagement and the expectation is that those would be completed prior to engagement start.
- Gather any documents which describe:
  - Your current analytics estate, including architecture, use cases and analytics applications.
  - Your data sources, data strategy and data roadmap.
  - An outline of what you plan to move to Qlik Cloud.
  - Your current processes and analytics operating model.
- Where a hybrid environment including a Client-Managed element of Qlik software will be used, Customer will ensure:
  - Servers have internet connectivity to qlikcloud.com.
  - Qlik Sense Enterprise Client-Managed versions are either the current version or one of the previous two major releases.
  - The Qlik Sense SaaS Readiness application has been run.
  - The Qlik Operations Monitor applications has been run.

### 2.3 Qlik Cloud Starter – Current QlikView Customer

Qlik Cloud Starter is intended for Customers who are currently active users of Client Managed QlikView and may include a combination of Consulting and Education Services.  Any Education Services below are subject to the Education Services Terms attached hereto and  at www.qlik.com/product-terms.

Services may include the following:

- **Deploy and Administer Qlik Sense SaaS Training** – Blended Training – Attendance by up to two (2) Customer personnel of the Deploy and Administer Qlik Sense SaaS Blended Training Course for 6 months (180 days).
- **Create Visualizations with Qlik Sense Training** – Blended Training – Attendance by up to five (5) Customer personnel of the Create Visualizations with Qlik Sense Blended Training Course for 1 year (365 days).
- **Data Modeling for Qlik Sense Training** – Blended Training - Attendance by up to two (2) Customer personnel of the Data Modeling for Qlik Sense Training Blended Training Course for 1 year (365 days**).**
- **Configuration of Tenant.** Qlik will provide configuration of Customer's Qlik Tenant including user authentication either via the Qlik IdP or to accept a compatible Customer IdP without the use of custom coding, configuration of SMTP, and configuration of Customer user authorization for governing Space access. Qlik will also configure standard Monitoring Applications and standard Demonstration Applications and provide basic enablement to a Customer user on the monitoring of their new Qlik environment.
- **Current State Review.** Qlik will work with the Customer personnel to define a target solution design and high-level migration roadmap with the Customer. Qlik will assist with:
  - A Baseline inventory of existing Client Managed QlikView applications in one production environment using a Qlik Consulting SaaS readiness utility.
  - Identify and present opportunities, risks, and recommended mitigations for migration to Qlik Cloud consistent with leading practices.
- **Basic Application Development.** Qlik will work with Customer business users to understand their needs and specific application requirements. Based on this work, Qlik will define a layout and use cases for the application to support and create an application based on these requirements, working with business users to refine the application based on business user feedback. The application will include data from one (1) data source, up to three (3) source tables, up to ten (10) master measures, and up to five (5) million rows. The implementation of row or column level security is not included.
- **Advisory Presentation – Leading Practices. Qlik will provide a presentation for basic enablement on the following topics:**
  - Application Access for End Users.
  - Application Development Lifecycle including Publishing to Production.
  - Onboarding New Users.

- **Advisory Presentation – Contextualized Capabilities.** Qlik will provide a presentation in the context of goals shared by the Customer throughout the engagement on the capabilities and practices the Customer may wish to leverage on the QCS platform, and how the Customer might consider leveraging them to meet their objectives.

**Pre-Requisites**

- Acquisition of licenses for QCS or QGS SaaS platform.
- Customer will provide a named individual for registration to the instructor led training.
- Customer will provide access to relevant resources (IdP administrator, existing BI administrator, business analysts, BI developers, database administrator, data architect, etc.) as needed through the project.
- Customer will configure IdP, data sources and existing Qlik deployments as needed in a timely manner to support implementation.
- Technical prerequisites and source/target setup instructions will be shared at the start of the engagement and the expectation is that those would be completed prior to engagement start.
- Gather any documents which describe:
  - Your current analytics estate, including architecture, use cases and analytics applications.
  - Your data sources, data strategy and data roadmap.
  - An outline of what you plan to move to Qlik Cloud.
  - Your current processes and analytics operating model.
- Where a hybrid environment including a Client-Managed element of Qlik software will be used, Customer will ensure:
  - Servers have internet connectivity to qlikcloud.com.
  - Qlik Sense Enterprise Client-Managed versions are either the current version or one of the previous two major releases.
  - The Qlik Sense SaaS Readiness application has been run.
  - The Qlik Operations Monitor applications has been run.

## 3. AutoML Starter Service

Qlik will engage with Customer to deliver an enablement-focused engagement resulting in a ML model developed against a Customer use-case in concert with Customer-personnel.

**3.1 Use-Case Selection:** Qlik will work with the Customer to identify a business use-case that is mutually agreed to be a good fit for modeling with Qlik AutoML. Specific activities will include:

- Assessment of desired use cases including the amount of data and complexity of data engineering required to achieve good results with an ML model will be carried out with the Customer.
- Qlik and Customer will agree on the use-case for this engagement ("Target Use Case") based on a quick analysis of benefits to the business, feasibility, technical complexity, availability and viability of necessary data, and constraints of current software licensing. The selected use-case will be the focus of the creation of the Qlik AutoML Model ("Target ML Model") to be delivered during this engagement.

**Assumptions:**

- Customer has one or more business use-cases identified that they believe will benefit from the application of ML modeling using Qlik AutoML. Details about the use-case including expected benefits and impact as well as the necessary data sources and transformations should be available.

**Start Criteria:**

- A kickoff meeting between Qlik and all relevant Customer stakeholders required to speak to the business and technical requirements, and other interested parties is scheduled at a mutually agreed upon time and duration.
- Customer will have identified a individual(s) who will be primarily responsible for working with Qlik consultants on the creation of the "Target ML Model" and provided the necessary contact information prior to the start of the engagement.
- Customer is currently using a licensed and fully functional instance of Qlik Cloud that has been configured and integrated to the extent required to conduct this engagement. Configuration of the Qlik Cloud SaaS tenant and integration with Customer systems including IDP are out of scope for this engagement.

**Acceptance Criteria**

- The Target Use Case will be selected as mutually agreed between Qlik and Customer following activities described in section 6.1 of this document.

**3.2 Enablement-focused ML Model Development:** Qlik will work with the Customer to establish a schedule for the presentation of enablement content pertaining to Qlik AutoML which Qlik will provide during the course of this engagement. Qlik and Customer will iterate through the development of the "Target ML Model" such that model development activities will coincide with the most recent enablement content presented in a working session following the presentation of enablement content. The Customer may take additional actions between working sessions to further develop the model, and Qlik will review progress and address questions, or issues encountered prior to presenting the subsequent enablement materials. Specific activities may include:

- Establish a mutually agreed-upon schedule for the presentation of structured online enablement content around the preparation and use of Qlik AutoML. The schedule may not exceed more than four (4) weeks in total duration unless otherwise mutually agreed.
- Iterative development of the "Target ML Model" through a series of working sessions of appropriate duration to complete the model development activities that correspond to the most recently consumed enablement content. The engagement may not exceed fifteen (15) working sessions. Working sessions will typically range from 30 to 60 minutes.

- Delivery and overview of the final working model with key Customer stakeholders following the completion of all working sessions. The efficacy and accuracy of the model will be significantly dependent on the quality and relevance of the data provided to train the model. The “Target ML Model” will function as expected in relation to its ability to leverage training data to make predictions against an applied data set. The accuracy of the model in its ability to predict future outcomes cannot be guaranteed.

**Assumptions:**

- Customer will make personnel with a working knowledge of relevant data and data sources available as needed through the course of the engagement to help ensure that the necessary data to train the model is available and appropriately engineered for consumption.
- Data engineering activities to manipulate or transform Customer data are out of scope for this engagement. Qlik Professional Services has the ability to provide these services for an additional fee if desired.

**Start Criteria:**

- Completion of Use-Case Selection
- The assigned Qlik Resource has been provided sufficient access to the Customer’s Qlik tenant and any data or business documentation necessary.

**Acceptance Criteria**

- The “Target ML Model” that conforms to the description in section 6.2 has been developed in collaboration with Customer personnel.

## C. Consulting Services- Talend Products

Consulting Services- Talend Products refers to consulting services provided in connection with the data integration products identified below.

### 1. Talend Cloud Starter Service

Qlik will work with the Customer to provide mentorship and deployment expertise to initiate a first data management use case in Customer’s Talend Cloud environment. Qlik will setup and install Talend Studio as the development environment and one Remote Engine where developed artifacts will be deployed and executed. Qlik will provide documentation of the performed installation and configuration and a sample Talend Job or a Talend Job design template for the initial use case.

Talend Cloud Starter Service is initiated with a kickoff meeting where Qlik will work with Customer’s main point of contact to prioritize the areas to address and to validate all prerequisites are met. Following the kickoff meeting, a Qlik Consultant will work towards a three-step plan that includes the following services:

**Step 1**: Set-up and configuration of Customer’s Talend Cloud tenant:

- Installation and configuration of Talend Studio for up to two users.
- Review connectivity to sources (up to three systems) and targets (up to two systems).
- Installation and configuration of one Remote Engine for remote execution.
- Creation of a test job, scheduling the job, job promotion to preferred execution engines for final installation/configuration validation.
- Documentation including a write up of installation/configuration.

**Step 2:** Application of best practices from the Talend Reference Architecture to Customer’s designated environment.

**Step 3:** Enablement and mentorship on core capabilities working with Content.

- Review of Talend Cloud Administration and Operational functions.
- Review of Software Development Life Cycle (SDLC) capabilities.
- Creation of a Sample Talend Job or a Job Design Template based on the agreed initial use case.
- Overview of additional Talend capabilities:
  - Talend Data Preparation
  - Talend Data Stewardship

**Prerequisites:**

All necessary equipment, resources and personnel are available throughout the duration of the engagement. Documentation including a description of the initial data management use case and associated requirements has been shared with Qlik.

Agreed engagement schedule.

- Downloads of Talend Software install packages have been completed.
- Required Talend product licenses are available.

Qlik recommends that the following Talend Academy trainings are completed prior to starting Talend Cloud Starter Services:

- Introduction to Talend Studio
- Talend Cloud Essentials
- Talend Data Integration Basics

### 2. Talend Data Management Starter Service

Qlik will work with the Customer to provide mentorship and deployment expertise to initiate first data integration or data quality use cases either on-premises, in the cloud, or in a hybrid architecture in Customer’s environment. Qlik will setup and install Talend Studio as the development environment and one Remote Engine where developed artifacts will be deployed and executed. Qlik will provide documentation of the performed installation and configuration and sample Talend Jobs or Talend Job design templates for the initial use cases.

Talend Data Management Starter Service is initiated with a kickoff meeting where Qlik will work with Customer's main point of contact to prioritize the areas to address and to validate all prerequisites are met. Following the kickoff meeting, a Qlik Consultant will work towards a four-step plan that includes the following services:

**Step 1:** Set-up and configuration.
**Step 2:** Application of best practices from the Talend Reference Architecture to Customer's designated environment.
**Step 3:** Enablement and mentorship on core capabilities working with Customer Data.
**Step 4:** Design, use case implementation and testing following a collaborative approach.

**Prerequisites:**

- All necessary equipment, resources and personnel are available throughout the duration of the engagement.
- Documentation including a description of the initial data integration or data quality use cases and associated requirements has been shared with Qlik.
- Agreed engagement schedule.
- Downloads of Talend Software install packages have been completed.
- Required Talend product licenses are available.

Qlik recommends that the following Talend Academy trainings are completed prior to starting Talend Cloud Starter Services:

- Introduction to Talend Studio
- Talend Cloud Essentials
- Talend Data Integration Basics
- Talend Data Quality Essentials

### 3. Talend Data Catalog Starter Service

Qlik will work with the Customer to provide mentorship and deployment expertise to initiate first metadata management use cases in Customer's environment. Qlik will provide documentation of the performed installation and of the Data Catalog in the Customer's environment along with the defined metadata models, business glossary, metadata management processes, security model based on the roles and responsibilities of the IT stakeholders.

Talend Data Catalog Starter Service is initiated with a kickoff meeting where Qlik will work with Customer's main point of contact to prioritize the areas to address and to validate all prerequisites are met. Following the kickoff meeting, a Qlik Consultant will work towards a four-step plan that includes the following services:

**Step 1:** Set-up and configuration:

- ○ Review and define Architecture, Design, and Infrastructure prerequisites.
- ○ Review connectivity to metadata sources (up to three systems).
- ○ Documentation including a write up of installation/configuration.

**Step 2**: Application of best practices from the Talend Reference Architecture to Customer's designated environment.
**Step 3:** Enablement and mentorship on core capabilities working with Customer metadata assets including harvesting, stitching, and building a metadata catalog:

- ○ Creation of a Business Glossary including taxonomy and structure
- ○ Definition of the logical and physical data models
- ○ Definition of the metadata model
- ○ Definition of the metadata repository structure
- ○ Definition of a security model based on roles of responsibilities of the IT stakeholders
- ○ Harvesting metadata
- ○ Stitching and establishing lineage
- ○ Definition of metadata processes
- ○ Testing and Validation of metadata sources and targets, metadata processes

**Step 4:** Establish alignment of information across the business and IT stakeholders.

**Prerequisites:**

- All necessary equipment, resources and personnel are available throughout the duration of the engagement.
- Documentation including a description of the initial metadata management use cases and associated requirements has been shared with Qlik.
- Agreed engagement schedule.
- Downloads of Talend Software install packages have been completed.
- Required Talend product licenses are available.

Qlik recommends that the following Talend Academy trainings are completed prior to starting Talend Cloud Starter Services:

- Talend Data Catalog Basics
- Talend Data Catalog Advanced

## D. Legacy Consulting Services

### 1. Customer Success Engineer (CSE).

**1.1 Customer Success Engineer (CSE).** A CSE or QDI CSE refers to a Qlik resource, who serves as a designated point of contact for up to six (6) technical contacts designated by a customer for technical support. CSE services are only available to customers who are current on their support or subscription obligations. Typical CSE activities include the following:

- Direct access to a CSE with knowledge of Customer's environment and priorities.
- Provide technical and solutions guidance to aid in the execution of the customers deployment.
- Conduct bi-annual platform reviews to provide recommendations on best practices.
- Provide ad-hoc assistance to address critical issues as they arise.
- Conduct a full Qlik Architecture review on a single production environment.
- Deliver standard Qlik workshops designed to provide insights and best practices on the Qlik platform. Standard workshops are typically 1-3 hours in duration.
- Provide basic install, configuration, and upgrade guidance. No hands-on keyboard or live assistance during actual upgrade.

**1.2 Extended Customer Success Engineer (Extended CSE)**. An Extended CSE refers to a Qlik resource, who serves as a designated point of contact for up to six (6) technical contacts designated by a customer for technical support. CSE services are only available to customers who are current on their support or subscription obligations. Typical CSE activities include the following:

- Direct access to a CSE with knowledge of Customer's environment and priorities.
- Provide technical and solutions guidance to aid in the execution of the customers deployment.
- Conduct up to 3 platform reviews per annum to provide recommendations on best practices.
- Conduct up to 2 Qlik Architecture reviews per annum on a single production environment.
- Deliver standard Qlik workshops designed to provide insights and best practices on the Qlik platform. Standard workshops are typically 1-3 hours in duration.
- Deliver Standard and Enhanced Qlik workshops designed to deliver insights on complex techniques and skills necessary to succeed with the Qlik platform. Enhanced Qlik workshops are typically 4 hours or more in duration.
- Provide basic install, config and upgrade guidance when needed.
- Deliver specialized technical knowledge, advanced troubleshooting, and coordination with additional Qlik resources, if needed, to facilitate problem resolution.
- Enhanced technical guidance and "hands on" assistance can also be provided through onsite visits and live interaction in support of technical issues resolution and upgrade/config support.

**CSE and Extended CSEs.** CSEs are available during regional business hours and are typically responsible for managing up to 6 customer accounts. Extended CSEs are available during regional business hours and are typically responsible for managing up to 3 customer accounts. In the event a CSE or Extended CSE is on leave or support is needed outside of regional business hours, inquiries will be directed to support specialists.

# QLIK® DATA PROCESSING ADDENDUM

This Data Processing Addendum including its Schedules 1, 2, 3 and 4 (the “**DPA**”), once executed and received by Qlik according to the instructions below, forms part of the Agreement between Qlik and the Customer (each defined below).

The Qlik party to this DPA is the Qlik entity that is the Qlik party to the Agreement. Only the Customer entity that is the party to the Agreement may sign this DPA. If the Customer entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA. The Customer’s signatory represents and warrants that he or she has the legal authority to bind the Customer to this DPA.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

In order for it to be effective, the Parties must (a) complete and sign the information block below with the Customer full legal entity details and signatory information and (b) sign Schedule 4 (2021 SCCs).

The Parties hereby agree from the Effective Date to be bound by the terms and conditions of this DPA.

| | | | |
|---|---|---|---|
| **Accepted and agreed to by Qlik** | | **Accepted and agreed to by the Customer** | |
| *Name of signatory* | Roy Horgan | *Customer legal name (include entity type, e.g., Inc., Ltd., etc.)* | |
| | | *Country of customer* | |
| *Position* | Senior Director, Privacy Counsel and Data Protection Officer | *Name of signatory* | |
| *Signature* | | *Position* | |
| *Date* | | *Signature* | |
| | | *Date* | |
| *Key privacy contact* | Roy Horgan, Senior Director, Privacy Counsel and Data Protection Officer<br>privacy@qlik.com | *Key privacy contact* | |

# SCHEDULE 1
# DATA PROTECTION OBLIGATIONS

This DPA is an agreement between the Customer and Qlik governing the Processing by Qlik of Customer Personal Data in its performance of the Services. Capitalized terms used in the DPA will have the meanings given to them in Section 1 below.

## 1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Agreement**" means either (i) the Qlik Customer Agreement or (ii) the Qlik OEM Partner Agreement, between Qlik and the Customer under which Qlik provides the applicable Services.

"**CCPA**" means the California Consumer Privacy Act, as amended, and its implementing regulations. The terms "**Business**" and "**Service Provider**" where used in this DPA addressing compliance under the CCPA will have the meanings given to them under the CCPA.

"**Client-Managed Deployment**" means a deployment of on-premise Qlik or Qlik Affiliate software managed and/or hosted by the Customer or by a Customer's third party cloud provider.

"**Consulting Services**" means any consulting services provided to the Customer by Qlik pursuant to the Agreement.

"**Customer**" means the customer legal entity which is a Party to the Agreement.

"**Customer Personal Data**" means Personal Data which Qlik Processes on behalf of the Customer in the performance of the Services, including, where applicable, Cloud Customer Content. It does not include Personal Data for which Qlik is a Controller.

"**Data Protection Law**" means, as amended from time to time, the Australia Privacy Act, the Brazil General Data Protection Law (LGPD), the Canada Personal Information Protection and Electronic Documents Act, the EU GDPR, the Israel Protection of Privacy Law, the Japan Act on the Protection of Personal Information, the Singapore Personal Data Protection Act, Swiss Federal Act on Data Protection, the UK Data Protection Act 2018 and UK General Data Protection Regulation, and the general consumer (non-industry specific) data privacy laws of the United States and its states (including, where applicable, the CCPA), and in each case only to the extent applicable to the performance of either Party's obligations under this DPA.

"**DPF**" means the EU-U.S. Data Privacy Framework, including the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework.

"**Effective Date**" means the date on which Qlik receives a validly executed DPA under the instructions above and always subject to the Customer having validly executed an Agreement.

"**EEA**" means, for the purpose of this DPA, the European Economic Area (including the European Union) and, for the purposes of this DPA, Switzerland.

"**EEA Customer Personal Data**" means Customer Personal Data that is subject to the EU GDPR.

"**EU GDPR**" means, in each case to the extent applicable to the Processing activities (i) Regulation (EU) 2016/679; and (ii) Regulation (EU) 2016/679 as amended by any legislation arising out of the withdrawal of the UK from the European Union.

"**Party**" or "**Parties**" means Qlik and the Customer, individually and collectively, as the case may be.

"**Personal Data**" means information relating to an identified or identifiable natural person or as otherwise defined under applicable Data Protection Law.

"**Personnel**" means a Party's employees or other workers under their direct control.

"**Qlik**" means the Qlik Affiliate which is party to the Agreement.

"**Qlik Cloud Customer Content**" means information, data, materials, media, or other content to the extent it includes Customer Personal Data that is, by, on behalf of or upon the instructions of the Customer, uploaded into and residing in Qlik Cloud which Qlik or a Qlik Affiliate Processes on behalf of the Customer.

"**Qlik Cloud**" means a subscription-based, hosted solution provided and managed by Qlik or an Affiliate under an Agreement.

"**Qlik DPF Companies**" means the U.S. Affiliates of the Group which participate in the DPF, found at https://www.dataprivacyframework.gov/s/.

"**Security Incident**" means unauthorized or unlawful destruction, loss, alteration or access to, or disclosure of, Customer Personal Data that is in Qlik's possession or under Qlik's control in its performance of the Services. It does not include events which are either (i) caused by the Customer or Customer Affiliates or their end users or third parties operating under their direction, such as the Customer's or Customer Affiliate's failure to (a) control user access; (b) secure or encrypt Customer Personal Data which the Customer transmits to and from Qlik during performance of the Services; and/or (c) implement security configurations to protect Customer Personal Data; or (ii) unsuccessful attempts or activities that do not or are not reasonably likely to compromise the security of Customer Personal Data, including but not limited to unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Service(s)**" means, pursuant to an Agreement, (i) Qlik Cloud, (ii) a Qlik Cloud trial, (iii) a Qlik Cloud presales proof-of-concept performed by Qlik, and/or (iv) Support Services and/or Consulting Services requiring Qlik personnel to access or otherwise Process on Customer's behalf either (a) Qlik Cloud Customer Content while within or originating from Qlik Cloud and/or (b) Customer Personal Data relating to a Client-Managed Deployment, and in each case, only as it relates to Processing by Qlik or a Qlik Affiliate of Customer Personal Data. Notwithstanding the foregoing, "Services" does not include, and accordingly, this DPA does not cover, (i) Qlik Cloud Customer Content which leaves Qlik Cloud, and/or (ii) Customer Personal Data stored in a Client-Managed Deployment, including but not limited to Customer Personal Data stored within self-hosted software.

"**Support Services**" means end user support provided by Qlik or an Affiliate to the Customer under the Agreement involving Processing by Qlik of Customer Personal Data either by way of (i) temporary remote access or screenshare, and/or (ii) receipt by Qlik or a Qlik Affiliate of Customer files via Qlik's support portal.

“**Swiss Customer Personal Data**” means Customer Personal Data that is subject to the Swiss Federal Act on Data Protection.

“**Termination Date**” means the termination or expiration of the relevant Service(s) under the Agreement between the Parties, or, in the case of a Qlik Cloud presales proof-of-concept or trial, the termination or expiration of that presales proof-of-concept or trial.

“**Third Country**” means a third country not deemed by the EU Commission, Swiss Federal Council or UK Information Commissioner, as applicable, to have an equivalent level of privacy protection to those jurisdictions.

“**UK Addendum**” means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner and laid before Parliament in accordance with S119A(1) Data Protection Act 2018 on 2 February 2022 but, as permitted by Section 17 of such Addendum, the format of the information set out in Part 1 of the Addendum shall be amended as set out in Section 5.4 of this DPA.

"**UK Customer Personal Data**" means Customer Personal Data that is subject to the UK General Data Protection Regulation.

“**2021 SCCs**” means the 2021 SCCs Module Two and the 2021 SCCs Module Three, collectively or individually, as applicable, published under EU Commission Decision 2021/914/EU for EU Personal Data transfers outside the EU to Third Countries not deemed by the EU Commission to have an equivalent level of privacy protection, included as Schedule 4. The terms “**2021 SCCs Module Two**” means the 2021 SCCs, module two (controller to processor), and “**2021 SCCs Module Three**” means the 2021 SCCs, module three (processor to processor).

"**Controller**", “**Data Subject**”, "**Processor**", “**Process/Processed/Processing**”, **“Subprocessor**” and “**Supervisory Authority**”, and analogous terms, will be interpreted in accordance with Data Protection Law.

## 2. PROCESSING BY QLIK OF CUSTOMER PERSONAL DATA

**2.1 Details of Processing.** The table below in this Section 2.1 sets out the Customer Personal Data Qlik may Process when providing the Services:

| | |
|---|---|
| **Nature/Activities/Purpose of Processing** | Processing of Customer Personal Data by the Customer in Qlik Cloud and/or for Support or Consulting Services. |
| **Frequency and Duration of Processing** | From time to time during the term of the Services under the Agreement or, in the case of a Qlik Cloud presales proof-of-concept or trial, the term of that proof-of-concept or trial. Duration of Processing and retention period shall be the duration of the Services unless Customer Personal Data is deleted sooner. |
| **Types of Personal Data Processed** | Customer Personal Data uploaded to and residing in Qlik Cloud and/or otherwise Processed by Qlik to provide the Services. Customer Personal Data may include sensitive Personal Data if provided by the Customer. |
| **Categories of Data Subjects whose Personal Data is Processed** | Qlik will not be aware of what Personal Data the Customer may provide for the Services. It is anticipated that Data Subjects may include employees, customers, prospects, business partners and vendors of the Customer. |

**2.2 Purpose of Processing Customer Personal Data.** The Parties agree that either (a) the Customer is the Controller and Qlik is a Processor, or (b) Customer is the Processor and Qlik is a Subprocessor, in relation to the Customer Personal Data that Qlik Processes on the Customer’s behalf in the course of providing the Services. For the avoidance of doubt, this DPA does not apply to Personal Data for which Qlik is a Controller. Qlik will Process Customer Personal Data only to perform the Services and for no other purpose. If Qlik is required to Process the Customer Personal Data for any other purpose by applicable laws to which Qlik is subject, Qlik will, unless prohibited by such applicable laws and subject to the terms of this DPA, inform Customer of this requirement first. To the extent that the CCPA applies to the Processing of Customer Personal Data in the course of providing the Services, (i) Qlik is a Service Provider and the Customer is a Business in relation to Customer Personal Data, and (ii) without limiting any other term in this DPA or in the Agreement, Qlik shall not (a) sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic means, any Customer Personal Data to any third-party for monetary or other valuable consideration, (b) retain, disclose, or use any Customer Personal Data for any purpose (including any commercial purpose) other than the specific purpose of performing the Services, and/or (c) retain, use, or disclose any Customer Personal Data outside of the direct business relationship between the Customer and Qlik. Qlik hereby certifies that it understands the restrictions described in the previous sentence and shall comply with them. To the extent that any database registration requirements are required under local laws a result of Customer’s use of the Services, Customer warrants that it shall undertake any such legally required registrations.

**2.3 Disclosure of Customer Personal Data.** Unless otherwise provided for in this DPA, Qlik will not disclose to any third party any Customer Personal Data, except, in each case, as necessary to maintain or provide the Services, or, notwithstanding Section 5.7 below, as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order).

**2.4 Customer Personal Data for Support Services.** The Parties acknowledge that Qlik does not ordinarily require to Process Customer Personal Data on the Customer’s behalf to resolve a technical issue for Support Services. Accordingly;

2.4.1 the Customer shall use their best efforts to minimize any transfer of Customer Personal Data to Qlik for Support Services. Such efforts shall include but not be limited to removing, anonymizing and/or pseudononymizing Customer Personal Data in files prior to Processing by Qlik; and

2.4.2 Qlik's total liability in relation to the Processing of Support Services Customer Personal Data, whether in contract, tort or under any other theory of liability, shall not exceed US$20,000.

**2.5 Obligations of Qlik Personnel.** Qlik will ensure that Qlik Personnel required to access the Customer Personal Data are subject to a binding duty of confidentiality in respect of such Customer Personal Data and take reasonable steps to ensure the reliability and competence of such Qlik Personnel.

**2.6 Instructions.** Customer authorizes and instructs Qlik to Process Customer Personal Data for the performance of the Services. The Parties agree that this DPA and the Agreement are the Customer's complete and final documented Processing instructions to Qlik in relation to Customer Personal Data. The Customer shall ensure that its Processing instructions comply with applicable Data Protection Laws in relation to Customer Personal Data and that the Processing of Customer Personal Data in accordance with the Customer's instructions will not cause Qlik to be in breach of any relevant law. The Customer warrants that it has the right and authority under applicable Data Protection Law and any undertakings it may have entered into to disclose, or have disclosed, Customer Personal Data to Qlik to be Processed by Qlik for the Services and that the Customer has obtained all necessary consents and provided all necessary notifications required by Data Protection Law with respect to the Processing of Customer Personal Data by Qlik. The Customer will not disclose Customer Personal Data to Qlik or instruct Qlik to Process Customer Personal Data for any purpose not permitted by applicable law, including Data Protection Law. Qlik will notify the Customer if Qlik becomes aware that, and in Qlik's reasonable opinion, an instruction for the Processing of Customer Personal Data given by the Customer violates Data Protection Law, it being acknowledged that Qlik is not under any obligation to undertake additional work, screening or legal assessment to determine whether Customer's instructions are compliant with Data Protection Law.

**2.7 Assistance to the Customer.** Upon a written request, Qlik will provide reasonable cooperation and assistance necessary to assist the Customer, insofar as required by Data Protection Law and as it relates to Processing by Qlik for the Services, in fulfilling the Customer's obligations to respond to requests from Data Subjects exercising their rights (notwithstanding the Customer's obligations in Section 7) and/or to carry out data protection impact assessments. Qlik's Data Protection Officer and privacy team may be reached at privacy@qlik.com.

**2.8 Compliance with Data Protection Laws.** Each Party will comply with the Data Protection Laws applicable to it in relation to their performance of this DPA, including, where applicable, the EU GDPR.

## 3. SECURITY

**3.1 Security of Data Processing.** Qlik will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data against unauthorized or unlawful Processing and against Security Incidents. These measures will be appropriate to the harm, which might result from any unauthorized or unlawful Processing, accidental loss, destruction, damage or theft of the Customer Personal Data and having regard to the nature of the Customer Personal Data which is to be protected. At a minimum, these will include the measures set out in Schedule 2.

**3.2 Notification of a Security Incident.** Upon becoming aware of a Security Incident, Qlik or a Qlik Affiliate will notify the Customer without undue delay and take reasonable steps to identify, prevent and mitigate the effects of the Security Incident and to remedy the Security Incident to the extent such remediation is within Qlik's reasonable control. A notification by Qlik or a Qlik Affiliate to the Customer of a Security Incident under this DPA is not and will not be construed as an acknowledgement by Qlik of any fault or liability of Qlik with respect to the Security Incident.

**3.3 Notification Mechanism.** Security Incident notifications, if any, will be delivered to Customer by any means Qlik selects, including via email. It is the Customer's responsibility to ensure that it provides Qlik with accurate contact information and secure transmission at all times.

## 4. SUBPROCESSORS

**4.1 Authorized Subprocessors.** The Customer agrees that Qlik may use its Affiliates and other Subprocessors to fulfil its contractual obligations under this DPA or to provide certain Services on its behalf. The Qlik website lists Subprocessors that are currently engaged by Qlik to carry out Processing activities on Customer Personal Data (currently located at https://community.qlik.com/t5/Qlik-Technical-Bulletin-Blog/Qlik-Subprocessors-General-Data-Protection-Regulation-GDPR/ba-p/1572352). The Customer may subscribe to the list in order to receive Subprocessor updates.

**4.2 Subprocessor Obligations.** Where Qlik uses a Subprocessor as set forth in this Section 4, Qlik will (i) enter into a written agreement with the Subprocessor and will impose on the Subprocessor contractual obligations not less protective on an aggregate basis than the overall obligations that Qlik has provided under this DPA, including but not limited to, where applicable, incorporating the 2021 SCCs and/or the UK Addendum; and (ii) restrict the Subprocessor's access to and use of Customer Personal Data only to provide the Services. For the avoidance of doubt, where a Subprocessor fails to fulfil its obligations under any subprocessing agreement or any applicable Data Protection Law with respect to Customer Personal Data, Qlik will remain liable, subject to the terms of this DPA, to the Customer for the fulfilment of Qlik's obligations under this DPA.

**4.3 Appointing a New Subprocessor.** At least thirty (30) days before Qlik engages any new Subprocessor to carry out Processing activities on Customer Personal Data, Qlik will provide notice of such update to the Subprocessor list through the applicable website. If the Customer is entitled to do so under applicable Data Protection Law and as it relates to the Processing of Customer Personal Data by the Subprocessor, the Customer may make reasonable objections in writing to privacy@qlik.com within the 30-day period regarding the appointment of the new Subprocessor. After receiving such written objection Qlik will either: (i) work with the Customer to address the Customer's objections to its reasonable satisfaction, (ii) instruct the Subprocessor not to Process Customer Personal Data, provided that the Customer accepts that this may impair the Services (for which Qlik shall bear no responsibility or liability), or (iii) notify the Customer of an option to terminate this DPA and the applicable order form for Services which cannot be provided by Qlik without the use of the objected-to new subprocessor. If Qlik does not receive an objection from the Customer within the 30-day objection period, the Customer will be deemed to have consented to the appointment of the new Subprocessor.

## 5. EEA/UK THIRD COUNTRY DATA TRANSFERS

**5.1 Transfers of EEA Customer Personal Data.** For transfers of EEA Customer Personal Data by the Customer to Qlik, where the Qlik party to this DPA is in a Third Country not deemed under EEA Data Protection Law to provide an equivalent level of privacy protection to that in the EEA and is not one of the Qlik DPF Companies;

5.1.1 where the Customer is the Controller and Qlik a Processor of such EEA Customer Personal Data, such transfer(s) are subject to the 2021 SCCs Module Two; and/or

5.1.2 where the Customer is the Processor and Qlik a Subprocessor of such EEA Customer Personal Data (i.e., where the EEA Customer Personal Data contains EEA Personal Data of the Customer's customers where the Customer is a Processor), such transfer(s) are subject to the 2021 SCCs Module Three;

in each case, the 2021 SCCs Module Two and 2021 SCCs Module Three, as applicable, shall apply as set out in Schedule 4 and subject to the provisions of this DPA.

**5.2 Particulars regarding the 2021 SCCs.** The 2021 SCCs are particularized in Schedule 4. The Parties agree that, to the fullest extent permitted under the 2021 SCCs, (a) the aggregate liability of Qlik to the Customer under or in connection with the 2021 SCCs will be limited as set out in sections 2.4 and 8.3 of this DPA, and (b) any rights to audit pursuant to Clause 8.9 of the 2021 SCCs will be exercised in accordance with section 6 below.

**5.3 Swiss Customer Personal Data.** For transfers of Swiss Customer Personal Data by the Customer to Qlik where the Qlik party to this DPA is in a Third Country not deemed under the Swiss Data Protection Law to provide an equivalent level of privacy protection to that in Switzerland and the Qlik party is not one of the Qlik DPF Companies, the Parties agree that the 2021 SCCs shall apply as set out in Schedule 4 and as particularized in clauses 5.1 and 5.2 of this DPA, save that references (i) to the EU GDPR shall be replaced by the respective references and/or equivalent terms in the Swiss Federal Act on Data Protection, (ii) to the competent supervisory authority in Annex I. C. shall be replaced with the Swiss Federal Data Protection and Information Commissioner, and (iii) to Member State(s), the EU and the EEA shall include Switzerland.

**5.4 UK Customer Personal Data**. For transfers of UK Customer Personal Data by the Customer to Qlik where the Qlik party to this DPA is in a Third Country not deemed under UK Data Protection Law to provide an equivalent level of privacy protection to that in the UK and the Qlik party is not one of the Qlik DPF Companies, the Parties agree that the provisions of the UK Addendum shall apply to such transfers. In particular:

5.4.1 the Customer will be the data exporter, and Qlik the data importer;

5.4.2 the start date for transfers in Table 1 of the UK Addendum shall be the Effective Date unless otherwise agreed between the Parties;

5.4.3 the details of the Parties and their key contacts in Table 1 of the UK Addendum shall be as set out at the commencement of this DPA, and with no requirement for additional signature;

5.4.4 for the purposes of Table 2, the UK Addendum shall be appended to the 2021 SCCs as incorporated by reference into this DPA (including the selection of modules as specified in Section 5.1, the particulars as specified in Section 5.2 of this DPA and the selection and disapplication of optional clauses as set out in Schedule 4);

5.4.5 the appendix information listed in Table 3 of the UK Addendum is set out at the commencement of this DPA (List of Parties), in Section 2 (Description of Transfer) and in Schedule 2 to this DPA (Technical and Organisational Measures); and

5.4.6 for the purposes of Table 4, neither Party may end the UK Addendum as set out in Section 19 thereof.

**5.5 Alternative Lawful Transfer Mechanisms.** The Customer acknowledges that Qlik's obligations under EEA/UK Third Country lawful transfer mechanisms (e.g. the 2021 SCCs, DPF) under this DPA may be replaced by obligations under any successor or alternate EEA/UK Third Country lawful transfer mechanism adopted by Qlik which is recognized by the relevant EEA/UK/Swiss authorities. In such instances, the Parties shall not be required to re-execute this DPA as they have already agreed to such measures, and such obligations will be deemed automatically included in this DPA. Customer acknowledges that, in the event of DPF no longer lawfully holding an adequacy decision, as judged by relevant EU/UK/Swiss authorities, a notification under section 5.6 (b) may be by way of an update by Qlik to its DPA terms at https://www.qlik.com/us/legal/legal-agreements.

**5.6 Transfers to Qlik DPF Companies.** If the Qlik party to this DPA is one of the Qlik DPF Companies, Qlik agrees to apply the DPF Principles issued by the U.S. Department of Commerce, located at https://dataprivacyframework.gov ("DPF Principles") to Customer Personal Data that Customer transfers to Qlik that originates from the European Economic Area, United Kingdom, or Switzerland if that Customer Personal Data meets the definition of "personal data" or "personal information" in the DPF Principles ("DPF Customer Personal Data"). For clarity, Qlik agrees to (a) use DPF Customer Personal Data only to provide the relevant Service; (b) notify the Customer if Qlik determines that it can no longer apply the DPF Principles to DPF Customer Personal Data; and (c) upon such determination, cease use of DPF Personal Data or take other reasonable and appropriate steps to apply the DPF Principles to DPF Customer Personal Data.

**5.7 EEA/UK-US Transfers.** In response to the Court of Justice of the European Union's decision in Schrems II, Case No. C-311/18, and related guidance from Supervisory Authorities, the Parties acknowledge that supplemental measures may be needed with respect to EEA/UK-U.S. data transfers where Customer Personal Data may be subject to government surveillance. The Customer and Qlik agree that Customer's EEA/UK operations involve ordinary commercial services, and any EEA/UK-U.S. transfers of EEA Customer Personal Data contemplated by this DPA involve ordinary commercial information, such as employee data, which is not the type of data that is of interest to, or generally subject to, surveillance by U.S. intelligence agencies. Accordingly, Qlik agrees that it will not provide access to Customer Personal Data of an EEA/UK Customer transferred under this DPA to any government or intelligence agency, except where its legal counsel has determined it is strictly relevant and necessary to comply with the law or a valid and binding order of a government authority (such as pursuant to a court order). If a law enforcement agency or other government authority provides Qlik with a demand for access to such Customer Personal Data, Qlik will attempt to redirect the law enforcement agency to request the Customer Personal Data directly from the Customer. If compelled by law to provide access to such Customer Personal Data to a law enforcement agency or other government authority, and only after a determination of such is made by legal counsel, then Qlik will, unless Qlik is legally prohibited from doing so: (1) give Customer notice of the demand no later than five (5) days after such demand is received to allow Customer to seek recourse or other appropriate remedy to adequately protect the privacy of EEA/UK Data Subjects, and Qlik shall provide reasonable cooperation in connection with the Customer seeking such recourse; and (2) in any event, provide access only to such Customer Personal Data as is strictly required by the relevant law or binding order (having used reasonable efforts to minimize and limit the scope of any such access). This Section 5.7 does not overwrite the equivalent protection under the relevant EEA/UK Third

Country lawful transfer mechanism (e.g., 2021 SCCs), if applicable.

**5.8 EEA Qlik Cloud Storage Capability.** For the avoidance of doubt, although the Customer may select (where available) the region in which its Qlik Cloud Customer Content resides, including the EU, the ability to retain Qlik Cloud Customer Content (including Customer Personal Data) solely in-region is subject to how the Customer's users of Qlik Cloud share and use applications and other technical particulars.

## 6. AUDITS

**6.1 Audit Reports.** Qlik and/or its relevant Affiliate(s) conduct periodic audits of its controls of relevant systems and processes (e.g., ISO 27001, SOC II), which may include systems and processes involved in the Processing of Customer Personal Data. These audits (i) occur on a regular, recurring basis, (ii) are performed according to the standards and rules of the relevant regulatory or accreditation body, (iii) are paid for by Qlik/its Affiliate(s), and (iv) produce an audit report ("Audit Report"). The Customer may request, and Qlik shall provide (subject to a NDA, where necessary), such Audit Report(s) or extracts thereof, where applicable to the Services, in order to satisfy the Customer of Qlik's compliance with statutory Processor obligations (e.g., Article 28 EU GDPR).

**6.2 Additional Information and Audits.** Where the information provided in the Audit Reports is not reasonably sufficient to demonstrate compliance by Qlik of its statutory Processor obligations in relation to the applicable Services, the Parties shall discuss in good faith any additional audits reasonably required by the Customer. Such additional audits, if agreed, must be (i) conducted by a third party agreed to by the Parties, (ii) carried out at the Customer's cost, (iii) be conducted in a manner undisruptive to the business of Qlik and its Affiliates, (iv) be conducted subject to the terms of an applicable non-disclosure agreement, and (v) not prejudice other confidential information (including but not limited to Personal Data) of Qlik, its Affiliates or its other customers.

**6.3 Subprocessor Audits.** If the Customer's request for information relates to a Subprocessor, or information held by a Subprocessor which Qlik cannot provide to the Customer itself, Qlik will promptly submit a request for additional information in writing to the relevant Subprocessor(s). The Customer acknowledges that information about the Subprocessor's previous independent audit reports is subject to agreement from the relevant Subprocessor, and that Qlik cannot guarantee access to that Subprocessor's audit information at any particular time, or at all.

## 7. ACCESS AND DELETION OF CUSTOMER PERSONAL DATA

**7.1 Access and Deletion of Qlik Cloud Customer Content during the Agreement.** Customer is responsible for any data minimization before inputting Customer Personal Data and for executing any requests to access, retrieve, correct and/or delete Qlik Cloud Customer Content (including any Customer Personal Data therein). Qlik will, as necessary to enable the Customer to meet its obligations under Data Protection Law, provide the Customer via availability of Qlik Cloud with the ability to access, retrieve, correct and delete through to the Termination Date its Qlik Cloud Customer Content in Qlik Cloud. The Customer acknowledges that such ability may from time to time be limited due to temporary service outage for maintenance or other updates to Qlik Cloud. To the extent that the Customer, in its fulfilment of its Data Protection Law obligations, is unable to access, retrieve, correct or delete Customer Personal Data in Qlik Cloud due to prolonged unavailability (for example, exceeding 10 working days) caused by an issue within Qlik's control, upon written request from the Customer, Qlik will where possible use reasonable efforts to provide, correct or delete such Customer Personal Data. The Customer acknowledges that Qlik may maintain backups of Qlik Cloud Customer Content, which would remain in place for approximately third (30) days following a deletion in Qlik Cloud. The Customer remains solely responsible for the deletion, correction and accuracy of its Qlik Cloud Customer Content and will be solely responsible for retrieving such Qlik Cloud Customer Content to respond to Data Subject access requests or similar requests relating to Customer Personal Data. If Qlik receives any such Data Subject request, Qlik will use commercially reasonable efforts to redirect the Data Subject to the Customer.

**7.2 Access and Deletion of Customer Personal Data on Termination of the Agreement**. By the Termination Date, the Customer will have deleted all Qlik Cloud Customer Content Personal Data, unless prohibited by law, or the order of a governmental or regulatory body. Notwithstanding the foregoing, after the Termination Date and upon the Customer's written request Qlik will provide reasonable assistance to the Customer to securely destroy or return any remaining Customer Personal Data. The Customer acknowledges that Customer Personal Data may be stored by Qlik after the Termination Date in line with Qlik's data retention rules and back-up procedures until it is eventually deleted. To the extent that any portion of Customer Personal Data remains in the possession of Qlik following the Termination Date, Qlik's obligations set forth in this DPA shall survive termination of the Agreement with respect to that portion of the Customer Personal Data until it is eventually deleted.

## 8. MISCELLANEOUS

**8.1 Entire Agreement.** This DPA and the Agreement, where referenced, contain the entire agreement regarding the subject matter thereof and supersede any other data protection/privacy agreements and communications between the Parties concerning the Processing by Qlik of Customer Personal Data in Qlik's performance of the Services.

**8.2 Effect of this DPA.** Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the Parties, including the Agreement and this DPA, the terms of this DPA will control as it relates to Processing of Customer Personal Data. If the Parties have entered into a Business Associate Agreement, that Business Associate Agreement shall govern with respect to U.S. "PHI" as defined thereunder. In the event of a conflict between this DPA and the applicable EEA/UK Third Country lawful transfer mechanism (e.g., 2021 SCCs, DPF)), the relevant Third Country lawful transfer mechanism terms/principles will prevail. This DPA is effective from the Effective Date and only if and for so long as Qlik provides Services under the Agreement. This DPA will terminate, unless otherwise terminated by the Parties, on the Termination Date.

**8.3 Liability.** Subject to Section 2.4.2, the total combined liability of either Party towards the other Party, whether in contract, tort or under any other theory of liability, shall be limited to that set forth in the Agreement as well as any disclaimers contained therein. Any reference in such section to the liability of a Party means the aggregate liability of that Party under the Agreement and this DPA.

**8.4 Third Party Rights.** This DPA shall not confer any rights or remedies to any other person or entity other than the Parties except as to enable the Data Protection Law rights of Data Subjects of Customer Personal Data under this DPA.

**8.5 Updates to this DPA.** Qlik may modify the terms of this DPA, such as to account for future changes in Data Protection Law to enable the continued Processing of Customer Personal Data to carry out the Services and shall do so by way of updating the DPA terms on www.qlik.com. Any future changes to this DPA published by Qlik on its website will become effective once published and shall supersede any previous DPA between the Parties, insofar and only to the extent that those changes (i) are to account for changes under Data Protection Law, which may include to account for revised guidance from a Supervisory Authority, or (ii) to enable an EEA/UK Third Country lawful transfer mechanism, as contemplated under Section 5.5, or (iii) are not less favorable to the Customer (for example, to permit further data types of Customer Personal Data to be uploaded to Qlik Cloud). The Customer is therefore encouraged to keep up to date with these DPA terms at www.qlik.com.

## SCHEDULE 2
## TECHNICAL AND ORGANIZATIONAL MEASURES

Qlik shall undertake appropriate technical and organizational measures for the availability and security of Customer Personal Data and to protect it against unauthorized or unlawful Processing and against accidental or unlawful loss, destruction, alteration or damage, and against unauthorized disclosure or access. These measures, listed below, shall take into account the nature, scope, context and purposes of the Processing, available technology as well as the costs of implementing the specific measures and shall ensure a level of security appropriate to the harm that might result from a Security Incident. Some of the measures below apply to Qlik's general IT infrastructure/practices and may not necessarily apply to Qlik Cloud. While Qlik may alter its measures in line with evolving security practices and risks, and with due regard to the nature of the Processing, Qlik will not materially decrease the overall protections of the Customer Personal Data below the aggregate standard of the measures in this Schedule 2. Customers should stay up to date with Qlik's security measures by visiting its security resources available at www.qlik.com.

**1. Access Controls to Premises and Facilities.** Qlik maintains technical and organizational measures to control access to premises and facilities, particularly to check authorization, utilizing various physical security controls such as ID cards, keys, alarm systems, surveillance systems, entry/exit logging and door locking to restrict physical access to office facilities.

**2. Access Controls to Systems and Data.** Qlik operates technical and organizational measures for user identification and authentication, such as logs, policies, assigning distinct usernames for each employee and utilizing password complexity requirements for access to on-premises and cloud-based platforms. In addition, user access is established on a role basis and requires user management, system or HR approval, depending on use. Second-layer authentication may be employed where relevant by way of multi-factor authentication. User access for sensitive platforms is subject to periodic review and testing. Qlik's IT control environment is based upon industry-accepted concepts, such as multiple layers of preventive and detective controls, working in concert to provide for the overall protection of Qlik's computing environment and data assets. To strengthen access control, a centralized identity and access management solution is used to manage application access. Qlik uses on-boarding and off-boarding processes to regulate access by Qlik Personnel.

**3. Disclosure Controls.** Qlik maintains technical and organizational measures to transport, transmit and communicate or store data on data media (manual or electronic). For certain data transfers, bearing in mind the risk and sensitivity of the data, Qlik may employ encrypted network or similar transfer technologies. Personnel must utilize a dedicated or local VPN network to access internal resources and/or industry-standard authentication and secure communication mechanisms to access cloud-based systems. Logging and reporting are utilized for validation and review purposes. Third party Subprocessors are subject to privacy and security risk assessments and contractual commitments.

**4. Input Controls.** Qlik maintains measures in its general IT systems for checking whether relevant data has been entered, changed or removed (deleted), and by whom, such as by way of application-level data entry and validation capabilities. and reporting is utilized for validation and review purposes. For Qlik Cloud Customer Content, other than as provided for under this DPA, the Customer is solely responsible for entry, alteration and removal (deletion) of any of its Qlik Cloud Customer Content in Qlik Cloud and, to respect the security and integrity of the Customer Personal Data, Qlik does not monitor Qlik Cloud Customer Content for regular entries, alterations or removals (deletion) by the Customer or its users in its use of the Services.

**5. Job Controls.** Qlik uses technical (e.g., access controls) and organizational (e.g., policies) measures to delineate, control and protect data for which the Qlik is the Controller or the Processor. Qlik records and delineates the data types for which it is a Controller or a Processor in its record of processing activities under Article 30 (2) EU GDPR.

**6. Separation Controls.** Qlik uses segregation standards and protocols between production, testing and development environments of sensitive platforms. Additionally, segregation of data is further supported through user access role segregation.

**7. Availability Controls.** Qlik maintains measures to assure data availability such as local and/or cloud-based back-up mechanisms involving scheduled and monitored backup routines, and local disaster recovery procedures. Qlik may supplement these with additional security protections for its business, for example malware protection. Additionally, data centers of a critical nature are required to submit to periodic 3rd party evaluation of operating effectiveness for significant controls ensuring data availability. Relevant systems and data center locations are protected through the use of industry-standard firewall capabilities.

**8. Other Security Controls.** Qlik maintains (i) regular control evaluation and testing by audit (internal and/or external), on an as-needed basis, (ii) individual appointment of system administrators, (iii) user access by enterprise IDP, (iv) binding policies and procedures for Qlik's Personnel, and (v) regular security and privacy training. Policies will clearly inform Personnel of their obligations (including confidentiality and associated statutory obligations) and the associated consequences of any violation.

**9. Certifications**. Qlik has, at the time of the Effective Date, and shall maintain, certifications regarding SOC 2 Type II and ISO 27001 or their equivalents, which may change over time in line with evolving security standards.

**10. Cloud Specific Measures.** Further security measures relating to Qlik Cloud are set out in the Qlik Cloud Information Security Addendum. Security measures in relation to Talend Cloud are set out in the Talend service description guide at https://www.qlik.com/us/legal/product-terms .

## SCHEDULE 3
## SUBPROCESSORS

**For Qlik offerings:**

**Qlik Third Party Subprocessors:**

- Amazon Web Services
- MongoDB
- Salesforce
- Grazitti SearchUnify
- Microsoft
- Persistent
- Altoros
- Ingima
- ISS Consult
- Galil
- Google Firebase
-

**For Talend offerings:**

**Talend Third Party Subprocessors:**

- Amazon Web Services
- Microsoft Azure
- MongoDB
- GitHub
- Intercom
- Atlassian
- Microsoft
- Proofpoint Secure Share
- Salesforce

**Affiliates:**

| Affiliates | Country |
|---|---|
| QlikTech International AB, Talend Sweden AB | Sweden |
| QlikTech Nordic AB | Sweden |
| QlikTech Latam AB | Sweden |
| QlikTech Denmark ApS | Denmark |
| QlikTech Finland OY | Finland |
| QlikTech France SARL, Talend SAS | France |
| QlikTech Iberica SL (Spain), Talend Spain, S.L. | Spain |
| QlikTech Iberica SL (Portugal liaison office), Talend Sucursal Em Portugal | Portugal |
| QlikTech GmbH, Talend Germany GmbH | Germany |
| QlikTech GmbH (Austria branch) | Austria |
| QlikTech GmbH (Swiss branch), Talend GmbH | Switzerland |
| QlikTech Italy S.r.l., Talend Italy S.r.l. | Italy |
| Talend Limited | Ireland |
| QlikTech Netherlands BV, Talend Netherlands B.V. | Netherlands |
| QlikTech Netherlands BV (Belgian branch) | Belgium |
| Blendr NV | Belgium |
| QlikTech UK Limited, Talend Ltd. | United Kingdom |
| Qlik Analytics (ISR) Ltd. | Israel |
| QlikTech International Markets AB (DMCC Branch) | United Arab Emirates |
| QlikTech Inc., Talend, Inc., Talend USA, Inc. | United States |
| QlikTech Corporation (Canada), Talend (Canada) Limited | Canada |
| QlikTech México S. de R.L. de C.V. | Mexico |
| QlikTech Brasil Comercialização de Software Ltda. | Brazil |
| QlikTech Japan K.K., Talend KK | Japan |
| QlikTech Singapore Pte. Ltd., Talend Singapore Pte. Ltd. | Singapore |
| QlikTech Hong Kong Limited | Hong Kong |
| Qlik Technology (Beijing) Limited Liability Company, Talend China Beijing Technology Co. Ltd. | China |
| QlikTech India Private Limited, Talend Data Integration Services Private Limited | India |
| QlikTech Australia Pty Ltd, Talend Australia Pty Ltd. | Australia |
| QlikTech New Zealand Limited | New Zealand |

. Further details are available at, and any changes shall be published to, https://community.qlik.com/t5/Qlik-Technical-Bulletin-Blog/Qlik-Subprocessors-General-Data-Protection-Regulation-GDPR/ba-p/1572352.

## SCHEDULE 4
## 2021 SCCs

*Controller to Processor (Module 2) or Processor to Processor (Module 3)*

### 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 personal 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 I.A (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 I.A (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 I.B.

(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) 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); and

(viii) Clause 18(a) and (b).

(ix) [If the data exporter is a controller:] Clause 8.1(b)

(x) [If the data exporter is a processor:] Clause 8.1(a), (c) and (d) and Clause 8.9 (f) and (g);

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

***Clause 4***

**Interpretation**

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

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

(e) 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 I.B.

### *Clause 7*

### [not used]

## 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.

**MODULE TWO: Transfer controller to processor**

#### 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 I.B, 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 II 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 I.B. 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 II. 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 I.B.

### 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 benefitting 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.

**MODULE THREE: Transfer processor to processor**

### 8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

### 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 I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

### 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 rectify or erase 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 I.B. 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 controller 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, they 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 subject. 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 or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out in Annex I.B.

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by 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 benefitting 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 of Regulation (EU) 2016/679;

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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

**MODULE TWO: Transfer controller to processor**

(a) 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 at least thirty (30) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

**MODULE THREE: Transfer processor to processor**

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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.

(d) 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.

(e) 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

**MODULE TWO: Transfer controller to processor**

(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.

**MODULE THREE: Transfer processor to processor**

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: 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.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Sweden.

### *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 Sweden.

(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.

## ANNEX I

### A. LIST OF PARTIES

**MODULE TWO: Transfer controller to processor**
**MODULE THREE: Transfer processor to processor**

**Data exporter(s):**

Name: The Customer, as defined in the Agreement.

Address: The address of Customer specified in the Agreement, DPA and/or applicable order form(s) as applicable.

Contact person's name, position, and contact details: The name, position, and contact details of the Customer's contact person specified in the table at the commencement of this DPA.

Activities relevant to the data transferred under these Clauses: transfer of Customer Personal Data, as defined in the DPA, for Processing by the data importer.

Signature and date: [insert signature and date]

Role: controller (module two) or processor (module three).

**Data importer(s):**

Name: Qlik, as defined in the Agreement.

Address: The address of Qlik specified in the Agreement, DPA and/or applicable order form(s) as applicable.

Contact person's name, position, and contact details: Roy Horgan, Senior Director, Privacy Counsel & Data Protection Officer, privacy@qlik.com.

Activities relevant to the data transferred under these Clauses: Processing of Customer Personal Data, as defined in the DPA, on behalf of the data exporter.

Signature and date: [insert signature and date]

Role: processor (module two) or subprocessor (module three).

## B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

See the Details of Processing table at the commencement of this DPA.

*Categories of personal data transferred*

Customer Personal Data as defined in the DPA. See the Details of Processing table at the commencement of the DPA.

*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*

See the Details of Processing table at the commencement of the DPA. Applied restrictions or safeguards are set out in the DPA.

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)*

See the Details of Processing table at the commencement of the DPA.

*Nature of the processing*

See the Details of Processing table at the commencement of the DPA.

*Purpose(s) of the data transfer and further processing*

For the purposes of enabling the data exporter to use the Services in accordance with the Agreement.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

In accordance with any retention periods controlled by the Customer, or if such retention periods are controlled by Qlik, in accordance with the Agreement and the DPA.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

Qlik's Subprocessor details are set out at Schedule 3 to the DPA.

## C. COMPETENT SUPERVISORY AUTHORITY

*Identify the competent supervisory authority/ies in accordance with Clause 13*

The Competent Supervisory Authority of the EU Member State in which the data exporter is established, based on the list available at https://edpb.europa.eu/about-edpb/about-edpb/members_en. In case of ambiguity, this will be the Competent Supervisory Authority of Sweden:

Integritetsskyddsmyndigheten
Drottninggatan 29
5th Floor
Box 8114
104 20 Stockholm

Tel. +46 8 657 6100, Fax +46 8 652 8652, Email: imy@imy.se, Website: http://www.imy.se/

## ANNEX II

### TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

These are as listed in Schedule 2 of the DPA.

## ANNEX III

### LIST OF SUB-PROCESSORS

The Controller has authorised the use of the sub-processors listed in Schedule 3 of the DPA, as updated from time to time.

# Education Services Product Terms

These Education Services Product Terms (“Education Product Terms”) provide a description of the Education Services offerings below. The Education Services offerings are governed by these Education Product Terms and any existing agreement between Qlik and the Customer which governs the provision of education services, or if none, the Consulting and Education Services Terms attached hereto and at www.qlik.com/legal-agreements (“Services Agreement”). In the event of any conflict between the Services Agreement and these Education Services Product Terms, these Education Services Product Terms will prevail. Any reference to Education Terms in a customer agreement shall be deemed to be a reference to the Education Product Terms and the Services Agreement collectively.

## 1. Training Courses

### 1.1. Training Course Delivery Options

Qlik currently offers its training courses (“Training Courses”) via the following delivery options:

| Training Course Delivery Options | Description |
|---|---|
| (1) Public Classroom | Live public classroom training at a designated Qlik location. Courses are delivered by Qlik authorized instructors. |
| (2) Private Classroom | Live private classroom training at a designated Qlik location. Courses are delivered by Qlik authorized instructors. |
| (3) Onsite Classroom | Live private classroom training onsite at Customer’s location. Courses are delivered by Qlik authorized instructors. |
| (4) Virtual Public Classroom | Live virtual public training using online (in the cloud) class environment consisting of live interactive webcasts, hands-on labs and mentoring. Courses are delivered by Qlik authorized instructors. |
| (5) Virtual Private Classroom | Live virtual private training using online (in the cloud) class environment consisting of live interactive webcasts, hands-on labs and mentoring. Courses are delivered by Qlik authorized instructors live through a virtual environment. |
| (6) Blended Learning Courses | Virtual Public or Private Classroom and self-placed learning |

### 1.2. Requirements for Onsite Classroom Training Courses

Customer is responsible for compliance with all of the following requirements for all Onsite Classroom Training Courses:

- Maximum number of participants for Onsite Classroom Training Courses is 10 participants.
- Each participant must have a dedicated computer for the duration of the course.
- The course location must be of adequate size (as determined by Qlik) to support the actual number of participants attending the course.
- The course location facility must be equipped with the following:

(1) Projection equipment, including but not limited to an overhead projector, LCD panel, high-definition television or equivalent display device with a diagonal display area of 40 inches (one meter).

(2) A projection screen with a diagonal measurement of at least six feet (two meters).

(3) Room darkening for display purposes to be operated by instructor.

(4) A blackboard, whiteboard, or flipchart of at least 10 square feet (or one square meter).

(5) If indicated by Qlik for a particular course, a high-speed Internet connection (wired or wireless), of approximately 1.5Mbps of bandwidth so that all participants may connect in the same room.

## 2. Training Services

Qlik currently offers the following training services (“Training Services”):

### 2.1. Qlik Continuous Classroom (Qlik Hosted)

a. Qlik Continuous Classroom (Qlik Hosted) is self-service, on-line learning content hosted by Qlik. Access to Qlik Continuous Classroom (Qlik Hosted) (“QCCQH”), is provided on a subscription basis for the applicable subscription period, selected User type and authorized quantity of Users. Each User must be unique, named user, and User credentials may not be shared among individuals. Subject to the Users’ compliance with these Education Terms and the payment of the applicable fees, Qlik grants to such Users a personal, limited, non-assignable, non-exclusive, and non- transferable term license, without the right to sublicense, to access and view QCCQH solely for such Users’ personal training and education. “Users” shall mean Customer’s employees or FTE contractors. The QCCQH subscription date shall start on the date that Qlik delivers the QCCQH subscription registration to Customer or its authorized reseller.

b. QCCQH for Individuals Users. Each User shall access QCCQH via such User’s Qlik Account. User acknowledges and agrees that User’s Qlik Account is confidential and nontransferable and may not be shared with any other person or entity. Further, any use of User’s ULC to allow or permit another person or entity to access QCCQH shall terminate User’s license to QCCQH.

c. Corporate / Full Access Subscriptions

(i) Corporate / Full Access Qlik Continuous Classroom (Qlik Hosted) (Corporate QCCQH). Upon the purchase of Corporate QCCQH, Customer (through its administrator), shall be responsible to enable, via the Qlik Subscription Management Portal (“SMP”) for up to the amount of authorized quantity of Users.

(ii) Qlik Continuous Classroom for Professional Users – Basic Subscriptions (QCCPUB). If a Qlik software product subscription includes a subscription to Qlik Continuous Classroom for Professional Users – Basic Subscriptions, Customer (through its administrator), shall be responsible to enable the applicable licensed users via the SMP.

(iii) Customers are fully responsible for the proper use of the SMP, and any use of the SMP allowing or permitting (i) more than the authorized or licensed number of Users and (ii) any person (other than Customer’s authorized Users) or entity to access Corporate QCCQH or QCCPUB shall terminate Customer’s license to the applicable product.

d. QCCQH may include community forums, office hours, or other interactive features. Such features are provided by Qlik in its sole discretion, and Qlik makes no representation, warranty or covenant about the availability, content or timeliness of any such features. Users should refer to the Usage Guidelines for Qlik Continuous Classroom Interactive Forums for further information.

### 2.2. Qlik Continuous Classroom (Customer-Hosted)

a. Qlik Continuous Classroom (Customer Hosted) is self-service, on-line learning content hosted by Customer. Qlik Continuous Classroom (Customer Hosted) (QCCCH) is accessible only by the purchase of a QCCCH license by Customer for its Users. Subject to the Users’ compliance with these Education Terms and the payment of the applicable fees, Qlik grants to such Customer and its Users a personal, limited, non-assignable, perpetual, non-exclusive, and non-transferable license, without the right to sublicense, to use the videos, exercises, quizzes and instructional materials that are made available by Qlik in QCCCH solely for such Users’ personal training and education, Qlik in its discretion shall determine the content and medium of the components of QCCCH.

b. QCCCH Customers may host QCCCH on a web server or LMS system, provided that Customer is solely responsible for integration and/or implementation efforts for such hosting. Further, Customer is responsible to ensure that any third party hosting entity of QCCCH on its behalf is in compliance with these Education Terms.

c. For clarity, no interactive features, including but not limited to student forums and instructor office hours, are included with QCCCH. Under no circumstances may Customer resell or use QCCCH to offer or provide any training or education (whether or not for fee) to any third party, or to offer any training or education materials, instruction or courses that incorporate or relate in any way to QCCCH to any third party. Customer acknowledges and agrees that it is fully responsible for any changes, modifications, alterations or customizations it makes to QCCCH.

d. Updates to QCCCH are provided by Qlik only upon the purchase of QCCCH updates. QCCCH updates must be purchased within the 90-day period following the 1-year anniversary date of QCCCH purchase or last QCCCH updates purchased. Purchases of QCCCH updates made after such period shall require the purchase of all updates since the date of original QCCCH purchase or last QCCCH updates purchase.

## 2.3. Talend Academy

a. Talend Academy is self-service, online learning content hosted by Qlik. Access to Talend Academy, is provided on a subscription basis for the applicable subscription period as described on an applicable Order Form. Subject to the Users' compliance with these Education Terms and the payment of the applicable fees, Qlik grants to such Users a personal, limited, non-assignable, non-exclusive, and non- transferable term license, without the right to sublicense, to access and view Talend Academy solely for such Users' personal training and education. "Users" shall mean Customer's employees or FTE contractors. Talend Academy subscriptions begin on the Order Form Start Date and terminate upon the expiration of the subscription period.

(i) **Per Seat Subscription.** Access to Talend Academy with the Per Seat Subscription will be based on the number of seats of Talend Academy purchased on an applicable Order Form.

(ii) **All Users Subscription.** Access to Talend Academy with the All Users Subscription shall be based on (1) The quantity set forth on the Order Form ("per Seat"); (2) Equivalent to the sum of (a) the number of Named Users, (b) the number of Talend Data Catalog Concurrent Consumer Users, (c) two (2) times the number of Talend Data Catalog Concurrent Admin Users, and (d) ten (10) times the number of all Concurrent Users excluding Talend Data Catalog Concurrent Users; or (3) Unlimited, provided that Customer has purchased an Education Services subscription applicable to all Software and Cloud Users and Customer's annual fees for all Software and Cloud Products exceeds $200,000 (USD).

(iii) **Enhanced Talend Academy Subscription.** In conjunction with an active Talend Academy or Talend Success Subscription, Customer will be provided with a maximum number of "Private Instructor-Led Training Days" quarterly as set forth in the Order Form. Private Instructor-Led Training Days include course delivery from an experienced Talend Instructor as well as access to training materials and hands-on virtual lab environments. A training day is defined to be one calendar day of a course being delivered for up to eight (8) hours of instruction. Training must be conducted between 8:00 AM to 6:00 PM in the local time zone, Monday through Friday, excluding holidays. Course attendance is restricted to ten (10) attendees, unless otherwise agreed in writing with Qlik. Courses may be held online in a virtual environment or in-person onsite. Customer shall reimburse Qlik for all reasonable travel, accommodations, and out-of-pocket Qlik Expenses incurred in connection with any in-person onsite Private Instructor-Led Training Days in accordance with FAR 31.205-46 and the Federal Travel Regulation (FTR). Customer must provide Qlik their desired training schedule a minimum of 15 business days in advance of the desired delivery date. Customer must provide Qlik with written notification a minimum of 3 business days prior to the scheduled delivery date to cancel or reschedule an in-person course, and a minimum of 3 business days prior to the scheduled delivery date to cancel or reschedule an online course. Qlik reserves the right to reschedule an online course up to 5 working days prior to the commencement date of the applicable course and an in-person course up to 10 working days prior to the commencement date of the applicable course. Any unused "Private Instructor-Led Training Days" shall expire at the end of each quarter and shall not roll over to subsequent quarters within the Subscription Term. Additional "Private Instructor-Led Training Days" will be subject to a separate written agreement.

## 2.4. Custom Application Training (CAT) Services

a. Custom Application Training Services are training videos for Customer prepared by Qlik and hosted by Customer. Subject to payment of the applicable fees and Customer's compliance with these Education Terms, Qlik will provide to CAT Customers the training video(s) ("Videos") for Customer's designated Qlik Applications applicable to the level of CAT Services purchased by Customer. Customer acknowledges that the CAT Services levels designate the number of total content minutes of Videos provided by Qlik, and do not guarantee that any specific number of Videos shall be provided by Qlik. Customer acknowledges that Qlik makes available resources to perform the CAT Services based upon the date of Customer's order. Accordingly, to the extent permitted by law, in the event that the CAT Services have not been completed by Qlik, due to any request by Customer or delay by Customer, by the earlier of (i) six (6) months from the date of the initial kickoff meeting, or (ii) 12 months from Customer's CAT Services order (the "CAT Services Expiration Date"), any amounts Customer has paid for the CAT Services shall expire and shall be forfeited. No refunds shall be provided for any such amounts previously paid, and Qlik shall have no liability to perform, and shall not perform, any CAT Services following the CAT Services Expiration Date.

b. Each Video will be delivered to Customer in a mutually agreed format such as MP4 or html. Customer is responsible to attend a kickoff meeting with Qlik to establish the requirements gathering process for the CAT Services. Customer shall work with Qlik to complete all requirements documents for each Video, which may include in person or on-line or telephone meetings between Customer and Qlik personnel. Further, Customer shall provide access to all Customer business and technical personnel needed for requirements gathering, and shall reasonably cooperate with Qlik in the performance of the CAT Services and shall provide Qlik with the information, feedback, instructions, and access to applicable equipment necessary to enable the timely performance of the CAT Services by Qlik in the manner provided herein. Customer shall be responsible for the completeness and accuracy of all information, data material, logos, trademarks and other intellectual property provided by Customer or its authorized representatives to Qlik. Customer represents and warrants that it has the full legal rights to provide the information, data, material, logos, trademarks, and other intellectual property (collectively, the "Customer Materials") to Qlik for inclusion in, or with respect to, the CAT Services.

c. The CAT Services also include applicable training reference card templates ("Reference Cards"), best practices for launching app and communication ("Launch Kit") and access to Qlik's adoption measurement tools to monitor user adoption metrics (collectively, the "CAT Materials"). Qlik grants to Customer a non-exclusive, non-transferrable, non-assignable perpetual license to use each Video and the CAT Materials delivered by Qlik for Customer and its Users' training and informational use. Customer may copy, modify and distribute to its Users the Reference Cards and the Launch Kit for its Users training and informational use. Customer may not, rent, lease, distribute, sell, sublicense, transfer or use with any third party in any wayany of the Videos or the CAT Materials. Customer shall not remove or alter any copyright or other proprietary rights notice of Qlik and/or its licensors in or on the Videos or any CAT Materials. All CAT Materials (and the intellectual property rights associated therewith) are and will remain at all times the sole and exclusive property of Qlik and its affiliates and licensors.

d. Qlik grants to Customer a non-assignable, non-transferable and non-exclusive right to access and use the Introduction to Qlik Training Content Videos in the CAT Services Application provided by Qlik solely for such Customer's Users' training and informational use. The foregoing videos may not be reproduced, modified, rented, leased, distributed, sold, sublicensed, transferred or used by any third party. Customer shall not remove or alter any copyright or other proprietary rights notice of Qlik and/or its licensors in or on the Qlik Training Content Videos.

## 2.5. Blended Learning Courses

a. Blended Learning Courses are training courses consisting of Virtual Live Instructor-Led Training, self-paced modules and access to applicable modules of Qlik Continuous Classroom – Qlik Hosted during the duration of the Blended Learning Course. Blended Training Courses are available as public or private Training Courses.

b. Blended Learning Courses utilize Qlik Cloud. If Customer does not already have a Qlik Cloud tenant ("Customer Tenant"), then upon Customer's request, Qlik shall provide Blended Learning Course participants with access to a limited term tenant on Qlik Cloud ("Training Tenant"). Notwithstanding anything to the contrary set forth in the applicable Qlik Cloud terms of service, Blended Learning Course participants may use the Training Tenant only for instructional purposes in connection with the Blended Learning Course and for no other purposes whatsoever. Any violation of the foregoing or any other provisions of the applicable Qlik Cloud terms of service shall result in the termination of participant's access to the Training Tenant. The Training Tenant and all content included therein will be available to Customer for the duration of the applicable Blended Learning Course If Customer chooses to use a separately issued Qlik Cloud tenant ("Customer Tenant") for a Blended Learning Course, Customer is responsible to ensure that its subscription for the Customer Tenant is valid for the entirety of the Blended Learning Course term and is solely responsible for the removal of any and all of its own data from the Training Tenant; in no event shall Qlik be responsible for any such data removal.

c. Blended Learning Courses may include forums, live instructor webinars, or other collaborative and/or interactive features (collectively, "Blended Forums"). The Blended Forums will include interaction and collaboration with other Blended Learning Course participants. Accordingly, participants should not use any confidential, non-public, personally-identifiable or sensitive data in connection with Blended Learning Courses. Qlik has no responsibility or liability with respect to any content or data shared or used by any Blended Learning Course participant. Further, in connection with the Blended Learning Course and the Training Tenant, all Blended Learning Course participants must comply with the Qlik Cloud Acceptable Use Policy located attached hereto and at https://www.qlik.com/us/legal/product-terms.

d. Applied Data Analytics using Qlik Sense (ADAQS) Blended Learning Course.. In addition to the terms in this Section 2.4, the following shall apply to ADAQS Blended Learning Course: The maximum number of participants in a private ADAQS Training Course is fifty (50). Further, to confirm attendance at an ADAQS Training Course, each participant must confirm participation within the Introduction Tab in the Course Materials no later than Week 2 of the course. Upon the earlier to occur of (i) the end of Week 2 of the course or (ii) participant's confirmation, no requests to reschedule participation in a ADAQS Training Course will be permitted.

### 2.6. QDI and Gold Client Classroom Training

Subject to payment of the applicable fees and Customer's compliance with these Education Terms, Qlik will provide classroom training for up to five (5) participants on applicable Qlik Data Integration ("QDI") products or Qlik Gold Client. Additional classroom days may be purchased. Any multi-day training must be scheduled on consecutive days Training will generally follow the description below, but may change at Qlik's discretion based on duration of the training and needs of the customer.

a. **Replicate Training.** Replicate training includes an introduction to Replicate and Enterprise Manager and covers capabilities and features as well as database requirements, installation, tasks, source and target endpoints, troubleshooting, transformations, notifications and command line tools. Hands-on training is included.

b. **QDI for Data Warehouse Automation – Compose Training**. Compose Training includes an introduction to Compose and covers capabilities and features as well as an overview of data warehouse concepts, understanding business requirements, sources, business rules (transformations), installation, configuring connections and authorization, defining data models, mappings and transformations, creating and populating data warehouses and data marts, defining data marts and setting up scheduler and monitoring.

c. **QDI for Data Lake Creation – Compose Training**. Compose Training includes an introduction to Compose and covers capabilities and features as well as data pipeline controls, row level computations and lookup, types of provisioning, automatic schema evolution, archiving, source variables, generated code inspection, hive projects, project tuning, DevOps integration, and Customer specific use cases and general Q&A.

d. **Qlik Gold Client.** Gold Client classroom training is for project team members and includes an overview of the software, support access and portal and software security as well as a software demo, training to enable customer to copy additional data as needed, and access to Gold Client support portal containing all user guides and ability to submit support tickets.

## 3. Terms and Conditions

### 3.1. Payment

a. Proof of payment is required for all Education Services.. For Education Services other than CAT Services and Talend Academy, payment may also be made by direct credit card payment, or at Qlik's discretion, upon Qlik or its authorized reseller as applicable invoice. If Qlik invoices Customer for any Education Services, such invoices are due and payable by Customer within ten (10) days of t receipt. Unless specifically agreed to by the parties, payments shall not be contingent on an issuance of a purchase order by Customer. Late payments shall bear interest from the due date at theinterest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid. Qlik shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k). Any amounts payable by Customer to Qlik under any other agreement or arrangement, including but not limited to license or support fees, are not conditional on the delivery of Education Services hereunder. Customer is responsible for all travel or out- of-pocket expenses incurred by Customer's personnel participating in any Training Course.

b. For all Training Courses to be held at a non-Qlik location, Customer shall reimburse Qlik for all actual and reasonable travel, lodging and meal expenses incurred by Qlik to deliver such courses in accordance with FAR 31.205-46 and the Federal Travel Regulation (FTR). Ordering Activity shall only be liable for such travel expenses as approved by Ordering Activity and funded under the applicable ordering document (collectively, "Qlik Expenses").

### 3.2. Reserved

**a.** .

### 3.3. Training Courses Availability; Registration of Participants, Cancellation and Rescheduling

a. All Training Courses are subject to space availability and Qlik's scheduling requirements. Customer shall promptly complete all registration or information forms required for any Training Course. Prior to the start date of any Private or Onsite Training Course, Customer shall provide to Qlik the list of participants scheduled to attend such Training Course. In the event that a scheduled participant is unable to attend a Training Course due to illness or a new role at Customer, or if such participant is no longer employed by Customer, Customer may substitute another participant for such Training Course upon prior written notice to Qlik of such new participant's contact details.

b. Cancellations and requests by Customer to reschedule Public Classroom, Private Classroom, Onsite Classroom, Virtual Private or Virtual Public Classroom Training must be made at least three (3) business days prior to the applicable Training Course start date in order to receive a full refund (excluding any nonrefundable Qlik Expenses). If Customer has paid by Training Card, such refund shall be credited to Customer's applicable Training Card number. No refunds or credits whatsoever shall be granted in the event such cancellation or rescheduling request is made less than three (10) business days prior to the start date of the Training Course. Notwithstanding the forgoing, if Customer cancels any public or private training class purchased as part of a bundle combined with other training offerings (such as Qlik Continuous Classroom), the fees attributable to such class shall be placed on a Training Card that shall expire 1 year from the date the bundle was purchased.

c. Qlik reserves the right to reschedule or cancel a Training Course due to low enrollment or if necessitated by an emergency or other unforeseen circumstance. Customer shall be credited for the full amount paid by Customer for such course, which credit may be used before the expiration of the applicable Training Card Term or within ninety (90) days following the date of Qlik's notice of cancellation or rescheduling, whichever is later. Qlik shall not be liable for non-refundable travel arrangements made by Customer in the event of a course rescheduled or cancelled by Qlik or Customer.

### 3.4. Certification Vouchers

**a. Issuance and Availability**. Each Certification Voucher is valid for one (1) Certification Exam attempt by a named individual, regardless of the final score. Each Certification Voucher is valid for only one (1) Certification Exam attempt and cannot be used more than once. Certification Exams are either (i)Qlik Product certification exams or (ii) Talend Product certification exams, which are only available through Qlik's authorized third party exam providers ("Exam Providersr"). Certification Vouchers may be purchased directly from the Exam Providers, purchased directly by Customer, or included as part of a bundled offering purchased by Customer.

**b. Redemption, Replacement and Non-transferability**. Each Certification Voucher must be presented at the time of registration for a Certification Exam. All Certification Vouchers have an expiration date, which is distributed with the Certification Voucher code and are valid only from the date of issuance through such expiration date ("Certification Voucher Term"). Upon the expiration of the Certification Voucher Term, the Certification Voucher shall expire and shall be forfeited. Certification Vouchers may only be applied to Certification Exams and cannot be used for any other Education Services, exchanged for any Training Cards, or redeemed for cash. Qlik is not responsible for any lost, expired, or invalid Certification Vouchers, and no replacements shall be provided. Customer shall have no right to transfer or assign any Certification Voucher to any affiliate or third party.

## 3.5. Customer Obligations

a. If Qlik is to perform any Education Services at Customer's site or location, Customer shall carry and maintain public liability insurance and employers' liability insurance, covering its employees, suppliers and contractors engaged at its premises, in amounts no less than required by the applicable law. Customer shall be responsible to comply with all of Qlik's policies and procedures that have been identified to Customer, including but not limited to health and safety, access to Qlik's equipment and systems, and confidentiality (collectively, "Qlik Policies" or individually, a "Qlik Policy"). Qlik reserves the right to remove from any Training Course or refuse to admit to any Training Course any participant who is not in compliance with any Qlik Policy.

b. Customer agrees to provide timely feedback to Qlik following completion of each Training Course or applicable Training Service, which may include satisfaction forms, customer surveys or evaluations (collectively, "Feedback").To the extent that Customer provides any Feedback or any other suggestions, data, information, comments or ideas with respect to Qlik's products and services (individually and collectively "Contributions"), Customer acknowledges and agrees that any and all Contributions made by Customer or any of its participants shall be deemed the confidential and proprietary property of Qlik. Customer expressly assigns, transfers and conveys all right, title and interest in and to the Contributions to Qlik. Customer agrees that Qlik and its designees will be free to use, copy, modify, create derivative works, publicly display, disclose, distribute, license and sublicense through multiple tiers of distribution and licensees, incorporate and otherwise use and exploit the Contributions, including derivative works thereto, for any and all commercial and non-commercial purposes, without any liability or obligation to Customer whatsoever. Qlik acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

## 3.6. Access to Training Courses; Ownership

a. If required for any Training Course, Qlik shall provide the applicable participants with an evaluation version of the applicable Qlik proprietary software to use during a live public or private classroom Training Course for instructional purposes only (the "Training Software") and such right to use the Training Software shall automatically terminate upon conclusion of the applicable Training Course. Attendance at a Training Course does not entitle any Customer or participant to any license whatsoever to any Qlik Software.

b. In connection with the Training Services or a Training Course, Qlik may distribute to or make available for download by participants Qlik-branded Training Course materials, in printed form or other medium ("Course Materials"). Subject to Customer's compliance with these Education Terms and the payment of the applicable fees, Qlik grants to Customer a personal, limited, non-assignable, non-exclusive, and non-transferable right, without the right to sublicense, to use the Course Materials solely for Customer's personal training and education.

c. Customer may not copy, reproduce, modify, rent, lease, distribute, sell, sublicense, transfer or use in any way except for in accordance with the limited right granted herein the Course Materials, the Training Services, Training Courses or any part thereof. Customer may use the information contained in the Course Materials, the Training Services and the Training Courses solely for education purposes only and may not disclose or make available to any person any information contained therein, except to others who have also rightfully received the same Course Materials, Training Services or Training Courses from Qlik. Except for the limited right to use granted herein, all rights in and to the Training Courses, Training Services and the Course Materials, and all copies thereof, are retained by Qlik and its licensors, including, without limitation, all patent rights, copyrights, trademark rights and trade secret rights. Customer shall not remove or alter any copyright or other proprietary rights notice of Qlik and/or its licensors in or on the Course Materials. All Training Services, Training Courses and Course Materials and the intellectual property rights associated therewith are and will remain at all times the sole and exclusive property of Qlik and its affiliates and licensors, and Customer has no right, title or interest in or to the Training Services Training Courses, Course Materials or the intellectual property associated therewith.

d. Certain Education Services require Customer to have sufficient Internet access. Qlik is not responsible for Customer's inability to access any such Education Services due to User's failure to have adequate Internet or bandwidth capabilities, or for any failure of the Internet or other communications or connectivity networks, or any disruptions or inaccessibility caused by third party sites, software or hardware.

## 3.7. Verification

Customer understands that Qlik may contact Customer, using the information provided by Customer, and that Qlik may verify such contact information in accordance with Qlik's then current privacy policy. Qlik has no obligation to allow Customer to use or access the Training Services, any Training Course and/or the Course Materials, unless Qlik is satisfied, in its discretion, that Customer is a bona fide trainee, that Customer has all necessary valid Customer licenses, if any, that Customer has paid the applicable fees foruse of the Training Services, Training Courses and/or Course Materials, and that the information provided by Customer to Qlik in registering for the Training Services, Training Courses and/or Course Materials is current, accurate and

## 3.8. General

a. Qlik may assign all or part of the Education Services to be performed hereunder to an affiliate or third party so long as Qlik shall remain liable for the actions and services provided by such affiliate or third parties. Qlik retains the right to assign, reassign and substitute personnel at any time. Provided that Qlik has used reasonable efforts to provide a suitable replacement (which shall always be subject to Qlik personnel availability), Qlik shall not be liable in the event of non-availability of any personnel due to death, leave, illness, family emergency, change of position, termination of employment or subcontract, or other similar reasons.

b. Qlik may at any time and from time to time non-materially modify the terms and conditions hereunder, provided that any such modification will be prospective only and not retroactive, that is, any such modification will not affect Education Services or Training Cards purchased prior effective date of such revision.

# Information Security Addendum – Qlik Cloud

This Information Security Addendum for Qlik Cloud ("Security Addendum") amends the agreement between Qlik and the Customer referencing this Addendum and governing use of Qlik Cloud ("Agreement"). To the extent of any conflict between the Agreement and this Security Addendum with respect to Qlik Cloud, this Security Addendum shall control.

## Security Program

Qlik recognizes that security is a fundamental consideration for Qlik Cloud customers and maintains a comprehensive documented security program based on ISO 27001 under which Qlik implements and maintains physical, administrative and technical safeguards designed to protect the confidentiality, integrity, availability and security of Qlik Cloud and Customer Content (the "**Security Program**") as set forth below.  Qlik utilizes infrastructure-as-a-service cloud providers (each, a "Cloud Infrastructure Provider") and provides Qlik Cloud using storage hosted by the applicable Cloud Infrastructure Provider. Qlik regularly tests and evaluates its Security Program and may review and update its Security Program as well as this Security Addendum from time to time consistent with industry standards.

### 1. Definitions

**"Customer Content"** means information, data, media or other content provided by Customer (or any users authorized by Customer) for use with Qlik Cloud.

"**Qlik Cloud**" means a subscription-based, SaaS solution provided and managed by Qlik under this SaaS Addendum

"**Security Incident**" means any unauthorized or unlawful destruction, loss, alteration or access to, or disclosure of, Customer Content that is in Qlik's possession or under Qlik's control. It does not include events which are either (i) caused by the Customer or Customer affiliates or their end users or third parties operating under their direction, such as the failure to (a) control user access; (b) secure or encrypt Customer Content which the Customer transmits to and from Qlik during performance of the Services; and/or (c) implement security configurations to protect Customer Content; or (ii) unsuccessful attempts or activities that do not or are not reasonably likely to compromise the security of Customer Content, including but not limited to unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

### 2. Audits and Certifications

Qlik's information security management program used to provide Qlik Cloud is assessed by independent third-party auditors as described in the following audits and certifications ("**Third Party Audits**"), on an annual basis:

- AICPA SSAE 18 SOC 1 Type 2
- AICPA SSAE 18 SOC 2 Type 2 + HITRUST CSF Attestation
- ISO/IEC 27001:2013

## 3. Hosting Location of Customer Content

The hosting location of Customer Content is determined by the location of the production instance of Qlik Cloud in the region selected by Customer upon initial tenant creation.

## 4. Encryption

**4.1. Encryption of Customer Content.** Qlik encrypts Customer Content at-rest using AES 256-bit (or better) encryption. Qlik uses Transport Layer Security (TLS) 1.2 (or better) for Customer Content in-transit over untrusted networks.

**4.2. Encryption Key Management.** Qlik provides per-tenant encryption keys, where the keys are updated when a customer saves changes to files within their tenant. Qlik logically separates encryption keys from Customer Content.

**4.3. Customer-Managed Keys**. Qlik Cloud has customer-managed key functionality, which enables Customers to create and manage their own encryption keys.

## 5. System & Network Security

**5.1. Access Controls.** Qlik Cloud is a no-view service where Qlik's *internal* network and Qlik personnel are separate from the production environment. Qlik personnel do not have direct access to Customer's Content and will not, subject to legal obligations, access Customer Content unless Customer invites Qlik into its tenant. The responsibility and access to perform operations, troubleshooting and support activity for Qlik Cloud is limited and restricted to Qlik personnel responsible for site reliability. All Qlik personnel access to Qlik Cloud is via a unique user ID, consistent with the principle of least privilege, requires a VPN, as well as multi-factor authentication and passwords.

**5.2. Endpoint Controls.** For access to Qlik Cloud, Qlik personnel use Qlik-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Malicious Code (as defined below), and (iii) vulnerability management in accordance with Section 4.7.3 (Vulnerability Management).

**5.3. Separation of Environments.** Qlik logically separates Qlik Cloud production environments from development environments.

**5.4. Firewalls.** Qlik shall protect the Qlik Cloud service using industry standard firewall with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business-required. In addition, Qlik also utilizes WAF technology.

**5.5. Hardening.** Qlik Cloud is hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Addendum.

**5.6. Monitoring & Logging**

**5.6.1. Infrastructure Logs.** Monitoring tools or services, such as network-based IDS, are utilized to log certain activities and changes within Qlik Cloud. These logs are further monitored, analyzed for anomalies and are securely stored to prevent tampering for at least one year.

**5.6.2. User Logs.** Customer tenant user logs of certain user activities and changes within their Qlik Cloud tenant are available to Customer for preservation and analysis.

**5.7. Vulnerability Detection & Management**

**5.7.1. Anti-Virus & Vulnerability Detection.** Qlik Cloud leverages industry standard threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code (collectively, "**Malicious Code**"). Qlik does not monitor Customer Content for Malicious Code.

**5.7.2. Penetration Testing & Vulnerability Detection.** Qlik works with an independent third party to conduct penetration tests of Qlik Cloud at least once annually. Qlik also runs weekly vulnerability scans for Qlik Cloud using updated vulnerability databases.

**5.7.3. Vulnerability Management.** Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to Qlik Cloud. To assess whether a vulnerability is 'critical', 'high', or 'medium', Qlik leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

## 6. Administrative Controls

**6.1. Personnel Security.** Qlik conducts background checks on Qlik personnel as part of our standard hiring process, subject to local laws and regulations.

**6.2. Personnel Training.** Qlik maintains a documented security awareness and training program for Qlik personnel. Qlik personnel are also required to acknowledge and comply with key Qlik security policies.

**6.3. Qlik Risk Management & Threat Assessment.** Qlik's risk management process is modeled on ISO 27001. Qlik conducts an annual risk assessment, which includes Qlik Cloud, to review material changes in the threat environment and to identify potential control deficiencies in order to make recommendations for new or improved controls and threat mitigation strategies.

**6.4. External Threat Intelligence Monitoring.** Qlik reviews external threat intelligence, including US-Cert vulnerability announcements and other trusted sources of vulnerability reports. U.S.-Cert announced vulnerabilities rated as critical or high are prioritized for remediation in accordance with Section 5.7.3 (Vulnerability Management).

**6.5. Vendor Risk Management.** Qlik maintains a vendor risk management program for vendors that process Customer Content designed to ensure each vendor maintains security measures consistent with Qlik's obligations in this Security Addendum. A list of these subprocessor vendors may be found here.

## 7. Physical & Environmental Controls

**7.1. Cloud Environment Data Centers.** To ensure the Cloud Infrastructure Provider has appropriate physical and environmental controls for its data centers hosting the SaaS Service, Qlik regularly reviews those controls as audited under the Cloud Infrastructure Provider's third-party audits and certifications. Each Cloud Infrastructure Provider shall have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks. Such controls, shall include, but are not limited to, the following:

7.1.1. Physical access to the facilities is controlled at building ingress points;

7.1.2. Visitors are required to present ID and are signed in;

7.1.3. Physical access to servers is managed by access control devices;

7.1.4. Physical access privileges are reviewed regularly;

7.1.5. Facilities utilize monitor and alarm response procedures;

7.1.6. Use of CCTV;

7.1.7. Fire detection and protection systems;

7.1.8. Power back-up and redundancy systems; and

7.1.9. Climate control systems.

**7.2. Qlik Development Locations.** While Customer Content is not hosted at Qlik offices, Qlik's technical, administrative and physical controls for its development locations are covered by its ISO 27001 certification and includes the following:

7.2.1. Physical access is controlled at office ingress points;

7.2.2. Badge access is required for all personnel and badge privileges are reviewed regularly;

7.2.3. Visitors are required to sign in;

7.2.4. Inventory of Qlik-issued laptops and network assets;

7.2.5. Fire detection and sprinkler systems; and

7.2.6. Climate control systems

## 8. Incident Detection & Response

**8.1. Security Incident**. Upon becoming aware of a Security Incident, Qlik will notify the Customer and take reasonable steps to identify, prevent and mitigate the effects of the Security Incident and to remedy the Security Incident to the extent such remediation is within Qlik's reasonable control.

**8.2. Investigation.** In the event of a Security Incident as described above, Qlik shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Any logs determined to be relevant to a Security Incident, shall be preserved for at least one year.

**8.3. Communication and Cooperation.** Security Incident notifications, if any, will be delivered to Customer by any means Qlik selects, including via email. It is the Customer's responsibility to ensure that it provides Qlik with accurate contact information and secure transmission at all times. Qlik shall provide Customer timely information about the Security Incident to the extent known to Qlik, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Qlik to mitigate or contain the Security Incident, the status of Qlik's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Qlik personnel may not have visibility to the content of Customer Content, it may be unlikely that Qlik can provide information as to the particular nature of the Customer Content impacted, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of Qlik with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Qlik of any fault or liability with respect to the Security Incident.

## 9. Business Continuity and Disaster Recovery

**9.1 Business Continuity Plan/Disaster Recovery Plan.** As it relates to Qlik Cloud, Qlik is prepared to handle large business disruptions with its corporate business continuity program, which is driven by a Business Continuity Policy (BC Policy) and a Business Continuity Plan (BCP). BCP's are reviewed on an annual basis to confirm they are in accordance with the established policies and procedures. Qlik maintains a disaster recovery plan (DRP) to help ensure continued availability. The DRP is tested at least annually -date. Data backups are managed by a Cloud Infrastructure Provider to ensure redundancy. Primary and secondary backups are daily incremental and are encrypted in transit (SSL/TLS 1.2) and at rest (AES-256). Backups are retained in accordance with Qlik's internal Data Retention Policy.

## 10. Deletion of Customer Content

**10.1. By Customer.** Qlik Cloud provides Customer controls for the deletion of Customer Content.

**10.2. By Qlik.** Subject to applicable provisions of the Agreement and deletion of primary data by Customer, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "**retrieval period**" set forth in the Agreement, Qlik shall regularly delete backups of Customer Content.

## 11. Customer Rights & Shared Security Responsibilities

**11.1. Customer Audit and Inquiry Rights.**

**11.1.1.** Upon written request and at no additional cost to Customer, Qlik shall provide Customer, and/or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing Qlik's compliance with its obligations under this Security Addendum in the form of, as applicable, (i) Qlik's ISO 27001 certificate, (ii) Qlik's SOC 2 Type II audit report and SOC 1 Type II audit report (iii) Qlik's most recently completed industry standard security questionnaire, such as a SIG or CAIQ, and (iv) architecture and technical overview documentation for the Service (collectively, "**Audit Reports**"). Audit Reports are considered Qlik's Confidential Information.

**11.2. Shared Security Responsibilities.** Without diminishing Qlik's commitments in this Security Addendum, Customer agrees:

**11.2.1.** Qlik has no obligation to assess the content or accuracy of Customer Content, including to identify information subject to any specific legal, regulatory or other requirement.

**11.2.2.** Customer is responsible for managing and protecting its user roles and credentials, including but not limited to (i) ensuring that all users keep credentials confidential and not share such information with unauthorized parties, (ii) promptly reporting to Qlik any suspicious activities related to Customer's account (e.g., a user credential has been compromised), (iii) appropriately configuring ser and role-based access controls, including scope and duration of User access, taking into account the nature of its Customer Content, and (iv) maintaining appropriate authentication, password and logging controls;

**11.2.3.** To appropriately manage and protect any Customer-managed encryption keys to ensure the integrity, availability, and confidentiality of the key and Customer Content encrypted with such key.

**11.2.4.** Customer is responsible for the security of any and all third-party software or applications installed and utilized by the Customer in conjunction with Qlik Cloud.

# Qlik Cloud Acceptable Use Policy

This Qlik Cloud Acceptable Use Policy ("AUP") defines acceptable practices and prohibited uses relating to Qlik's network and systems that are used for hosting Qlik products and services or providing SaaS services (collectively, the "Services") by users ("You" or "Your"). The Services must be used in a manner consistent with the intended purpose of the Services, the terms of Your applicable agreement with Qlik for the products and/or services being hosted and this AUP. Qlik may non-materially modify this AUP by posting a revised version to www.qlik.com. By using the Services, You agree to the latest version of this AUP. For purposes of this AUP, "Qlik" includes QlikTech International AB and its affiliates, and Qlik may be referred to as "We" or "Our."

## 1. Security

- You agree to maintain appropriate security, protection and backup copies of any content that is included, transmitted, stored, published, displayed, distributed, integrated, or linked by You in the Services (collectively, "Content"). We will have no liability of any kind as a result of the deletion of, correction of, destruction of, damage to, loss of or failure to store or backup any Content.
- You may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include:
  - Unauthorized Access. Bypassing, circumventing, or attempting to bypass or circumvent any measures We may use to prevent or restrict access to the Services (or other accounts, computer systems or networks connected to the Services), including any attempt to probe, scan, or test the vulnerability of the Services or to breach any security or authentication measures used by the Services.
  - Reverse Engineering. Deciphering, decompiling, disassembling, reverse engineering or otherwise attempting to derive any source code or underlying ideas or algorithms of any part of the Services, except to the limited extent applicable laws specifically prohibit such restriction.
  - Falsification of Origin or Identity. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route, or attempting to impersonate any of Our employees or representatives.
  - Using manual or automated software, robotic process automation, devices, or other processes to harvest or scrape any content from the Services.
  - Denial of Service (DoS)/Intentional Interference. Flooding a System with communications requests so the System either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective, or interfering with the proper functioning of any System, including by deliberate attempts to overload the System.

## 2. No Illegal, Harmful, or Offensive Use or Content

- You may not use, or encourage, promote, facilitate or instruct others to use, the Services for any illegal (under applicable law), fraudulent, infringing or offensive use, or to transmit, store, display, distribute, post or otherwise make available content that is illegal (under applicable law), harmful, fraudulent, infringing or offensive. Prohibited activities or content include:

  - Illegal, Harmful or Fraudulent Activities. Any activities that are illegal, that violate the rights of others, that may be harmful to others, or that may be harmful to Our operations or reputation.
  - Infringing Content. Content that infringes or misappropriates the intellectual property or proprietary rights of others or that violates any law or contractual duty.
  - Offensive Content. Content that is illegal, harassing, libellous, fraudulent, defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable.
  - Harmful Content. Content or other computer technology that may damage, interfere with, surreptitiously intercept or disrupt the Service, including viruses, Trojan horses, spyware, worms, time bombs, or cancelbots.
  - Unsolicited Content. Content that constitutes unauthorized or unsolicited advertising, junk or bulk e-mail (“spamming”) or contains software viruses or any other computer codes, files or programs that are designed or intended to disrupt, damage, limit or interfere with the proper function of any software, hardware, or AUP March 2021 telecommunications equipment or to damage or obtain unauthorized access to any system, data, password, or other information of Ours or any third party.
  - Competitive Content. Attempting to collect and/or publish performance data for the purposes of benchmarking, or developing a product that is competitive with any Our product or services.

### 3. Our Monitoring and Enforcement

- We reserve the right, but do not assume the obligation, to monitor for, and investigate, any violation of this AUP or other misuse of the Services. Failure to comply with this AUP constitutes a material breach of the terms and conditions upon which You are permitted to use the Services, and at any time may result in Qlik taking any and all remedial actions in its sole discretion in accordance with the Contract Disputes Clause, up to and including:
  - Warnings;
  - Suspending or terminating access to the Services;
  - Removing, disabling or prohibiting access to content that violates this AUP and/or Your applicable agreement with Qlik; and/or
  - Legal proceedings against You.

We may report any activity that We suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

We take no responsibility for any material created or accessible on or through the Services and will not exercise any editorial control over such material. We are not obligated to monitor such material, but reserves the right to do so, as well as remove any content that We, in Our sole discretion, determine to be in violation of this AUP.

## 4. Reporting of Violations of this Policy

If You become aware of any violation of this AUP, You will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. Violation of this AUP may be reported to security@qlik.com.

## 5. Subdomains

If You are permitted to choose a Qlik subdomain name for use with Qlik Cloud, such subdomain name may not infringe or violate third-party intellectual property rights or include offensive, obscene, vulgar or other objectionable or unlawful language, and be unique enough to prevent confusion with other entities, brands or trademarks. We reserve the right (but shall have not obligation to) to monitor, reject, revoke or cancel any Qlik subdomain name that is not in compliance with this Policy or any applicable laws.

# Qlik® Cloud Government Terms of Service

## 1. Agreement

These Qlik Cloud Government Terms of Service ("Terms") are effective when (A) a Customer places an Order with the Qlik entity identified in Table 1 to this Agreement ("Qlik") or (B) an Authorized Reseller places an order on behalf of the Customer (each an "Order Form"), are by and between Qlik and the Customer specified in the Order Form. These Terms govern the Customer's access to and use of Qlik Cloud Government and related Qlik Products and Services as referenced on the applicable Order Form. If the Customer does not agree to the Terms, or to any part of the Agreement, or if the Terms are not incorporated into the Order Form, the Customer must not use Qlik Cloud Government.

## 2. Definitions

Unless defined elsewhere in this Agreement, the capitalized terms utilized in this Agreement are defined below.

"**Account Data**" means specific Customer Data is that exempt from the boundary established in Qlik's FedRAMP System Security Plan and permitted within Qlik corporate services.

"**Agreement**" means these Qlik Cloud Government Terms of Service, and any Order Form(s) between Qlik and Customer for the provision of Qlik Cloud Government and any applicable Qlik Software or Services used in connection with Qlik Cloud Government.

"**Authorized Third Party**" means any third party authorized by Customer to access and use Qlik Products.

"**Authorized Reseller**" means a reseller, distributor or other third party authorized by Qlik to sell Qlik Products or Services.

"**Authorized User**" means an employee or Authorized Third Party of Customer, who has been authorized by Customer to use the Qlik Products in accordance with the terms and conditions of this Agreement and has been allocated a license or user credentials.

"**Confidential Information**" means non-public information that is disclosed by or on behalf of a Party under or in relation to this Agreement that is identified as confidential at the time of disclosure or should be reasonably understood to be confidential or proprietary due to the nature of the information and/or the circumstances surrounding its disclosure. Confidential Information does not include information which, and solely to the extent it: (i) is generally available to the public other than as a result of a disclosure by the receiving Party or any of its representatives; (ii) was known or becomes known to the receiving Party from a source other than disclosing Party or its representatives without having violated any confidentiality agreement of the disclosing Party; (iii) is independently developed by the receiving Party without the use or benefit of any of the disclosing Party's Confidential Information; or (iv) was disclosed by the disclosing Party to a third party without an obligation of confidence. In any dispute concerning the applicability of these exclusions, the burden of proof will be on the receiving Party and such proof will be by clear and convincing evidence.

"**Consulting Services**" means any consulting services performed by Qlik under the terms of this Agreement and any applicable Order Form.

"**Content**" means information, data and metadata created, collected, processed, maintained, disseminated, disclosed or disposed of by or for the Customer in any medium or form provided by Customer or any Authorized User for use with Qlik Cloud Government.

"**Customer**" means any of the following third parties that is permitted by Qlik to use, license or access Qlik Cloud Government: (a) the federal government, a federal government department and/or United States federal governmental agency of the United States; (b) a state or local government or a state or local governmental department or agency located in the United States; (c) K-12 & Higher Education utilizing a Government Contracting Vehicle; (d) Healthcare vendors/hospitals (not payers) utilizing a government contracting vehicle; or (e) system integrators, contractors and companies doing work for the Government solely in connection with such work for a Government entity, in each case that has entered into this Agreement by electronically accepting the terms or by accessing or using the Qlik Products; or where an Order Form has been executed, then Customer means the entity identified on the Order Form. For clarity, a Customer may include the Government public safety agencies, tribal, territorial, federally funded research centers (FFRDCs), or lab entities.

"**Delivery Date**" means the date on which access to the Qlik Products is initially made available (via download or otherwise) to Customer or to the Authorized Reseller as applicable, which date may be specified in an Order Form.

"**Documentation**" means the then-current user documentation for the Qlik Products, including the product metrics available at www.qlik.com/product-terms.

"**Education Services**" means any training or education services performed by Qlik under the terms of this Agreement and any applicable Order Form.

"**Export Control Laws**" means export control laws and regulations of the U.S., E.U., and other governments, as well as regulations declared by the U.S. Department of the Treasury Office of Foreign Assets Control, the U.S. Department of Commerce, the Council of the E.U. and their counterparts under applicable law ("Export Control Laws"), including all end user, end-use and destination restrictions imposed by such Export Control Laws.

"**External Use**" means an Authorized Third Party's use of any Qlik Products, which are designated for external use in the Documentation, provided such use is solely in connection with Customer's business relationship with the Authorized Third Party.

"**FedRAMP**" means the Federal Risk and Authorization Management Program.

"**IP Claim**" means a claim brought by a third party alleging that the Qlik Products, as delivered by Qlik and used as authorized under this Agreement, infringes upon any third- party copyright, trademark or a patent.

"**Government**" means any an agency, department, territory, or instrumentality of the U.S. government or an agency, department, or instrumentality of a state, county, municipal, or local government located in the United States.

"**Order Form**" means an order form, statement of work or written document pursuant to which Customer orders Qlik Products or Services to be performed by Qlik and executed by the Parties or by Customer and an Authorized Reseller.

"**Party**" or "**Parties**" means Qlik and Customer, individually and collectively, as the case may be.

"**Platform Data**" means the statistical data and performance information, analytics, metadata, or similar information, generated through instrumentation and logging systems, regarding the operation of Qlik Cloud Government, including Customer's use of

Qlik Cloud Government.

"**Qlik Acceptable Use Policy**" means Qlik's then-current Qlik Cloud Acceptable Use Policy attached hereto.

"**Qlik Cloud Government**" means a subscription-based, hosted solution provided and managed by Qlik under this Agreement to which the Customer is being granted access via a website or other designated IP address.

"**Qlik Marks**" means Qlik's trademarks, service marks, trade names, logos, and designs, relating to Qlik Products, whether or not specifically recognized, registered or perfected, including without limitation, those listed on Qlik's website.

"**Qlik Products**" means Software and Qlik Cloud Government. Qlik Products do not include Services or early release, beta versions or technical previews of product offerings.

"**Rules of Behavior**" means Qlik's then-current Qlik Cloud Government Rules of Behavior for External Users (attached hereto available at https://www.qlik.com/us/legal/qlik-cloud-government-onboarding-terms.

"**Services**" means Support, Consulting Services or Education Services performed by Qlik under the terms of this Agreement and any applicable Order Form. Services does not include Qlik Cloud Government.

"**Software"** means the generally available release of the Qlik software, in object code form, initially provided or made available to Customer as well as updates thereto that Qlik elects to make available at no additional charge to all of its customers that subscribe to Support for the Software.

"**Subscription**" means access to and usage of Qlik Cloud Government subject to this Agreement.

"**Support**" means end user support and access to updates for the Qlik Products, which are provided by Qlik as part of a subscription for Qlik Products.

## 3. Customer Rights and Responsibilities

**3.1.** **Use of Qlik Cloud Government.** Customer directly, or through a Qlik Partner, may purchase a Subscription to Qlik Cloud Government. Qlik will provide the Customer and the Customer's Authorized Users with non-exclusive access to Qlik Cloud Government, provided any use of Qlik Cloud Government shall be (i) in accordance with the Documentation and this Agreement; and (ii) for the authorized scope and quantities which may be specified in an Order Form. Customer may use Qlik Cloud Government solely for the Customer's own internal governmental purposes.

**3.2.** **Use of Qlik Software**. Subject to the terms of this Agreement, in the event Customer licenses Qlik Software to support its transition to Qlik Cloud Government, Qlik grants to Customer a world-wide, non-exclusive, non-transferable and non-sublicensable right for its Authorized Users to access or use Qlik Software for Customer's internal business operations and for External Use, provided any use of Qlik Software shall be (i) in accordance with the Documentation and this Agreement; and (ii) for the authorized scope and quantities which may be specified in an Order Form.

**3.3.** **Services.** Qlik will support Qlik Cloud Government and related Qlik Software in accordance with Qlik's Public Sector Service Level Agreement attached hereto for Customer's subscription period. Qlik may provide Consulting or Education Services to Customer pursuant to this Agreement, any applicable product descriptions (available at www.qlik.com/product-terms) and any applicable Order Form.

**3.4.** **Restrictions.** Customer will not, nor permit nor authorize anyone to: (i) make any Qlik Products available to anyone other than Customer or its Authorized Users; (ii) offer, use, or otherwise exploit the Qlik Products whether or not for a fee, in any managed service provider (MSP) offering; platform as a service (PaaS) offering; service bureau; or other similar product or offering; (iii) input, process or store any classified data in Qlik Cloud Government; (iv) copy, decompile, disassemble or reverse engineer or otherwise attempt to extract or derive the source code or any methods, algorithms or procedures from the Qlik Products, except as otherwise expressly permitted by applicable law, or modify, adapt, translate or create derivative works based upon the Qlik Products; (v) alter or circumvent any product, key or license restrictions, or transfer or reassign a named user license or entitlement, in such a manner that enables Customer to exceed purchased quantities, defeat any use restrictions, or allows multiple users to share such entitlement to exceed purchased quantities; (vi) copy or create Internet "links" to Qlik Cloud Government or "frame" or mirror" any of the Qlik Cloud Government; (vii) permit direct or indirect access to or use of Qlik Cloud Government or Content in a way that circumvents any usage limit; (viii) use the Qlik Products if Customer is a competitor of Qlik; or (viii) access or use the Qlik Products in order to (a) build a competitive product or service, (b) build a product using similar ideas, features, functions or graphics of the Qlik Products, or (c) copy any ideas, features, functions or graphics of the Qlik Products.

**3.5.** **Content**. Customer acknowledges and agrees that it has sole responsibility: (i) to administer Authorized User access to its account on Qlik Cloud Government and the Content, (ii) for the input and administration of Content in Qlik Cloud Government, including deletion of Content, (iii) to ensure it has all rights necessary to use, transmit and display Content and for Qlik to host, store, adapt or integrate such Content as required to provide Qlik Cloud Government, (iv) for maintaining Content on the systems from which they are sourced and making backup copies of Content; and (v) to ensure that all Authorized Users abide by the Qlik Acceptable Use Policy and the Rules of Behavior while accessing Qlik Cloud Government. Customer hereby represents and warrants on behalf of itself and its Authorized Users that it has all of the rights in the Content necessary for the use, display, publishing, sharing and distribution of the Content and that such use of the Content under this Agreement does not violate any third-party rights, laws or this Agreement. Qlik is not responsible for the accuracy, completeness, appropriateness, copyright compliance or legality of any Content.

**3.6.** **Authorized Third Parties**. If Customer chooses to have an Authorized Third Party access Qlik Cloud on its behalf, including Qlik employees accessing Qlik Cloud Government at Customer's request, Customer acknowledges that Customer, and not Qlik, is solely responsible and liable for (i) the acts and omissions of such Authorized Third Party in connection with Qlik Cloud Government; (ii) any Content that Customer requests or instructs the Authorized Third Party to include in Qlik Cloud Government; and (iii) the issuance, removal and/or deactivation of the credentials issued for such Authorized Third Party.

**3.7.** **Security**. Qlik will use commercially reasonable, industry standard security measures in providing Qlik Cloud Government and will comply with such data security regulations applicable to Qlik Cloud Government. Qlik has implemented appropriate technical and procedural safeguards to protect and secure Content. Qlik Cloud Government is hosted and delivered from a data center operated by a third-party provider, which is solely responsible for the underlying infrastructure and hosting of Qlik Cloud Government. Qlik reserves the right to remove or update its third-party provider. Customer is solely responsible for any breach or loss resulting from: (i) Customer's failure to control user access; (ii) failure to secure Content which Customer transmits to and from Qlik Cloud Government; and (iii) failure to implement security configurations and encryption technology to protect Content.

**3.8.** **Data Privacy.** The terms of the Data Processing Addendum attached hereto ("DPA") are incorporated by reference when executed by Customer as set forth in the DPA and received by Qlik, and shall apply to the extent Content includes "Customer Personal Data" as defined in the DPA. Customer and Authorized Users are not permitted to store, maintain, or process payment card information or related financial information subject to Payment Card Industry Data Security Standards, Protected Health Information (as defined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)).

**3.9.** **Access**. Customer may only use Qlik Products activated with a product key or other credentials provided by Qlik or via an Authorized Reseller. Customer is solely and directly responsible (a) for maintaining the security of all keys, user IDs, passwords and other credentials, (b) for all activities taken by its Authorized Users or under any of its keys or credentials; (c) for Customer's and Authorized Users' compliance with this Agreement and applicable laws, including Export Control Laws; and (d) to promptly notify Qlik of any unauthorized use or access and take all steps necessary to terminate such unauthorized use or access. Customer will provide Qlik with such cooperation and assistance related to any unauthorized use or access as Qlik may reasonably request.

## 4. Term and Termination

4.1 **Term**. Customer's and its Authorized Users' access to Qlik Products and Services shall remain in effect, unless earlier terminated, for the applicable subscription term set forth in the Order Form for such subscription ("Term"). A Term may be renewed for renewal terms of the same duration at Qlik's then-prevailing rates for the applicable Qlik Products by executing a written order. If a Subscription is not renewed then Subscriptions shall automatically terminate at the end of the-then current Term.

4.2 **Termination for Breach**. The Customer may terminate this Agreement (without resort to court or other legal action) if Qlik fails to cure a material breach within thirty (30) days in accordance with FAR 552.212-4(m) or other similar law or regulation if applicable to the relevant Order Form.

4.3 **Termination for Cause**. Subject to 41 U.S.C. § 71 (Contract Disputes), FAR 52.233-1 (Disputes), applicable local law or regulation, and unless a remedy is otherwise ordered by a United States Federal Court, Qlik may terminate the Agreement if it is determined that the Customer failed to comply with the Terms. Customer may terminate the Agreement effective immediately upon written notice to Qlik if Qlik (A) fails to cure a breach of the Agreement within 30 days of notice of the breach, or (B) commits an uncurable material breach of the Agreement, or (C) terminates or suspend its business.

4.4 Qlik may terminate Customer's or any individual Authorized User's access to all or any part of Qlik Cloud Government at any time if required by applicable law, effective immediately, which may result in the forfeiture and destruction of all information within Customer's subdomain. If the Qlik Products are purchased through an Authorized Reseller, Qlik may terminate any right to use the Qlik Products pursuant to this Section in the event Qlik fails to receive payment for such Qlik Products.

4.5 **Termination for Convenience**. Customer may terminate the Agreement for its sole convenience in accordance with FAR 52.212-4(l) or similar law or regulation if the clause is applicable to the relevant Order Form.

4.6 **Effect of Termination**. Upon any termination or expiration of this Agreement, Customer and its Authorized Users' right to access and use the Qlik Products and Services shall automatically cease. No refunds or credits of any prepaid fees shall be granted in the event of any termination or expiration. All provisions of this Agreement which by their nature should survive termination shall survive termination, including, without limitation, ownership provisions, warranty disclaimers, indemnity and limitations of liability. Termination of this Agreement or any licenses or subscriptions shall not prevent either Party from pursuing all available legal remedies, nor shall such termination relieve Customer's obligation to pay all fees that are owed.

4.7 Qlik may, without limiting its other rights and remedies, suspend Customer's access to Qlik Cloud Government at any time if: (i) required by applicable law, (ii) Customer or any Authorized User is in violation of the terms of this Agreement, the Qlik Acceptable Use Policy and/or the Rules of Behavior, or (iii) Customer's use disrupts the integrity or operation of Qlik Cloud Government or interferes with the use by others. Qlik will use reasonable efforts to notify Customer prior to any suspension, unless prohibited by applicable law or court order.

## 5. Warranties; Disclaimer; Limitation of Liability

**5.1.** **Warranty.** Qlik warrants that Qlik Cloud Government will perform substantially in accordance with the applicable Documentation when used as authorized under this Agreement. This warranty will not apply (i) unless Customer notifies Qlik of a claim under this warranty within 30 days of the date on which the condition giving rise to the claim first appears, or (ii) the event giving rise to the warranty claim was caused by misuse, unauthorized modifications, or third-party hardware, software or services. Customer's exclusive remedy and Qlik's sole liability with regard to any breach of this warranty will be, at Qlik's option and expense, to either: (i) repair or replace the non-conforming portion of Qlik Cloud Government or (ii) terminate the affected portion of Qlik Cloud Government and refund Customer, on a pro rata basis, any unused, prepaid fees as of the termination effective date, but in no event less than one thousand U.S. dollars (USD $1,000).

**5.2.** **Consulting and Education Warranty.** Qlik warrants that Consulting Services and Education Services will be performed using reasonable care and skill consistent with generally accepted industry standards. For any claimed breach of this warranty, Customer must notify

Qlik of the warranty claim within thirty (30) days of Customer's receipt of the applicable Consulting Services or Education Services. Customer's exclusive remedy and Qlik's sole liability with regard to any breach of this warranty will be, at Qlik's option and expense, to either: (i) re-perform the non-conforming Consulting Services or Education Services; or (ii) refund to Customer the fees paid for the non-conforming Consulting Services or Education Services. Customer shall provide reasonable assistance to Qlik in support of its efforts to furnish a remedy for any breach of this warranty

**5.3.** **Disclaimer**. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE QLIK PRODUCTS AND SERVICES ARE PROVIDED "AS IS," "AS AVAILABLE" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES IMPLIED BY ANY COURSE OF PERFORMANCE OR USAGE OF TRADE, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. QLIK AND ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, PARTNERS, SERVICE PROVIDERS AND LICENSORS DO NOT WARRANT THAT: (I) THE QLIK PRODUCTS WILL BE AVAILABLE AT ANY PARTICULAR TIME OR LOCATION; (II) THE QLIK PRODUCTS WILL BE FREE OF DEFECTS OR ERRORS, (III) THE QLIK PRODUCTS ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS; (IV) THAT THE QLIK PRODUCTS WILL NOT HARM COMPUTER SYSTEMS; OR (V) THE RESULTS OF USING THE QLIK PRODUCTS WILL MEET CUSTOMER'S OR AUTHORIZED USERS' REQUIREMENTS. FURTHER, ANY PREDICTIVE SERVICES INCLUDED IN QLIK CLOUD ARE BASED ON CUSTOMER'S CONTENT AND INPUT INTO QLIK CLOUD AND SUCH SERVICES ARE NOT A GUARANTEE OF RESULTS OR FUTURE PERFORMANCE

5.4. **Limitation of Liability.** Except for: (i) Qlik's indemnification obligations hereunder; (ii) Customer's breach of Section 3.3 (Restrictions), or Section 3.8(c) (Export Control); or (iii) Customer's violation of Qlik's intellectual property rights, each Party's maximum cumulative liability for any claims, losses, costs (including attorney's fees) and other damages arising under or related to this Agreement, regardless of the form of action, whether in contract, tort (including but not limited to negligence or strict liability) or otherwise, will be limited to actual damages incurred, which will in no event exceed the greater of (a) one thousand dollars (USD $1,000); or (b) the aggregate amount of subscription fees paid by Customer for Qlik Cloud Government for the twelve month period immediately preceding the date upon which the events giving rise to such claim occurred.

5.5. **Exclusion of Damages**. EXCEPT FOR EITHER PARTY'S BREACH OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, IN NO EVENT SHALL EITHER PARTY BE LIABLE UNDER CONTRACT, TORT, STRICT LIABILITY, NEGLIGENCE, WARRANTY OR ANY OTHER LEGAL OR EQUITABLE THEORY WITH RESPECT TO THE SERVICES,INCLUDING FOR ANY LOST PROFITS, DATA OR CONTENT LOSS, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF GOODWILL, OR FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE, COMPENSATORY OR CONSEQUENTIAL DAMAGES OF ANY KIND WHATSOEVER, EVEN IF THE PARTY HAD BEEN ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES.

5.6. THE LIMITATIONS, EXCLUSIONS AND DISCLAIMERS CONTAINED IN THIS AGREEMENT ARE INDEPENDENT OF ANY AGREED REMEDY SPECIFIED IN THIS AGREEMENT AND WILL APPLY TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY AGREED REMEDY IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE. TO THE EXTENT THAT QLIK MAY NOT, AS A MATTER OF LAW, DISCLAIM ANY WARRANTY OR LIMIT ITS LIABILITIES, THE SCOPE OR DURATION OF SUCH WARRANTY AND THE EXTENT OF QLIK'S LIABILITY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. IF A WAIVER, RIGHT, OR REMEDY IS EXERCISED PURSUANT TO MANDATORY LAW, IT SHALL BE EXERCISED SOLELY FOR THE PURPOSE PROVIDED AND IN CONFORMANCE WITH THE PROCEDURES AND LIMITATIONS EXPRESSLY PROVIDED FOR BY SUCH LAW.

## 6. Intellectual Property Rights; Indemnification

**6.1.** **Ownership**. Customer retains all right, title and interest in and to all Content. Qlik retains all right, title and interest in and to the Qlik Products, Platform Data, and if applicable, all deliverables resulting from performance of Consulting Services, including all know-how, methodologies, designs and improvements to the Qlik Products, but excluding any Content incorporated into any such deliverable. Qlik hereby grants Customer a non-exclusive license to use any deliverables or work product that are the result of any Consulting Services in connection with Customer's authorized use of the Qlik Products.

6.2. **Retention of Rights**. No title or ownership of any proprietary or other rights related to Qlik Products is transferred or sold to Customer or any Authorized User pursuant to this Agreement. All intellectual property rights not explicitly granted to Customer are reserved and Qlik, its affiliates, and their respective suppliers or licensors, where applicable, retain all right, title and interest in and to the Qlik Products, including all intellectual property rights embodied therein, as well as to all Qlik Marks. Customer is not obligated to provide Qlik with any suggestions or feedback about the Qlik Products, but if Customer elects to do so, Qlik may use and modify this feedback for any purpose, including developing and improving the Qlik Products, without any liability, time limitation, restriction, or payment to Customer.

6.3. **Indemnification by Qlik**. Qlik shall have the right to intervene to defend, indemnify and hold Customer and its directors, officers, employees, agents, and permitted successors and assigns harmless from any damages and costs awarded against Customer and its directors, officers, employees, agents, successors and assigns as a result of an IP Claim. Qlik will not be liable for any IP Claim arising from or based upon: (i) any unauthorized use of, unauthorized access granted to or unauthorized distribution of the Qlik Products; and/or (ii) use of any Content with or in Qlik Cloud Government. If the Qlik Products become, or, in Qlik's opinion, is likely to become, the subject of an IP Claim, Qlik may, at its option and expense, either: (i) obtain the right for Customer to continue using the affected Qlik Products in accordance with this Agreement; (ii) replace or modify the Qlik Product so that it becomes non-infringing while retaining substantially similar functionality; or (iii) if neither of the foregoing remedies can be reasonably effected by Qlik, terminate this Agreement (without need for a ruling by a court or arbitrator) and refund Customer any prepaid fees covering the remainder of the term of the terminated subscription. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. THIS SECTION 6.3 STATES QLIK'S SOLE AND ENTIRE OBLIGATION AND LIABILITY, AND CUSTOMER'S SOLE AND EXCLUSIVE RIGHT AND REMEDY, FOR INFRINGEMENT OR VIOLATION OF INTELLECTUAL PROPERTY RIGHTS.

6.4. **Conditions.** Qlik's indemnification obligations hereunder are subject to: (i) prompt notification of a claim in writing to the indemnifying party; (ii) consent to allow Qlik to have control of the defense and any related settlement negotiations; and (iii) provision of information, authority and assistance as necessary for the defense and settlement of the IP Claim.

## 7. Fees; Payment and Taxes

7.1 Customer shall pay all fees due within thirty (30) days from the receipt date of Qlik's valid invoice therefor, unless otherwise stated on an Order Form. Fees are not subject to any right of offset or. Qlik shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k).. If the Customer fails to pay any Fee when due, then Qlik may charge Customer interest at the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid. In the event any use of Qlik Products exceeds purchased quantities ("Overage"), without limiting Qlik's other rights and remedies at law or in equity, Customer will be invoiced and shall pay for such Overage as specified in an Order Form.

## 8. Confidentiality

**8.1.** Each Party will hold in confidence the other Party's Confidential Information and will not disclose or use such Confidential Information except as necessary to exercise its express rights to perform its express obligations hereunder. Any Party's disclosure of the other Party's Confidential Information may be made only to those of its employees or consultants who need to know such information in connection herewith and who have agreed to maintain the Confidential Information as confidential as set forth herein. Notwithstanding the foregoing, a Party may disclose the other Party's Confidential Information to the extent that it is required to be disclosed in accordance with an order or requirement of a court, administrative agency or other governmental body, provided that such Party, to the extent permitted by law, provides the other Party with prompt notice of such order or requirement in order that it may seek a protective order. Each Party's confidentiality obligations hereunder will continue for a period of three (3) years following any termination of this Agreement, provided, however, that each Party's obligations will survive and continue in effect thereafter with respect to, and for so long as, any Confidential Information continues to be a trade secret under applicable law. Qlik recognizes that Customers may be subject to the Freedom of Information Act 5 U.S.C. 552 or other similar open records law which may require that certain information be released, despite being characterized as "confidential" by the vendor. The Parties acknowledge and agree that the Qlik Products and all pricing information are Confidential Information of Qlik.

## 9. General

**9.1.** **Entire Agreement; Severability; No Wavier; Headings**. This Agreement is the entire agreement between Customer and Qlik with respect to the Qlik Products and supersede all prior or contemporaneous communications and proposals (whether oral, written or electronic) between Qlik and Customer with respect to the Qlik Products, including any prior version of this Agreement. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable. The failure of either party to exercise in any respect any right provided for herein shall not be deemed a waiver of any further rights hereunder. In addition, this Agreement shall supersede any conflicting or contradictory terms contained in any purchase order, order form, or any other document Customer submits to any of Qlik's designated vendors in connection with a purchase of a subscription to the Qlik Products, and any such conflicting or contradictory terms will be of no force or effect. Failure to enforce any part of this Agreement shall not constitute a waiver of any right to later enforce that or any other part of this Agreement. The section and paragraph headings in this Agreement are for convenience only and shall not affect their interpretation.

9.2 **Governing Law; Jurisdiction**. This Agreement is governed by the Federal law of the United States, but excluding any conflict of law rules or the United Nations Convention on Contracts for the International Sale of Goods, the application of which is hereby expressly excluded. TO THE EXTENT AVAILABLE UNDER APPLICABLE LAW, CUSTOMER EXPRESSLY WAIVES ANY RIGHT TO A JURY TRIAL REGARDING DISPUTES RELATED TO THIS AGREEMENT.

9.3 **Early Release Products**. Qlik may, in its discretion, periodically provide certain Customers with an opportunity to test additional early release features or functionality in connection with Qlik Products. Customer may decline to participate in the testing of such additional features or functionality at any time. Customer acknowledges that such features or functionality are not considered part of the Qlik Products under this Agreement, are not supported, are provided "as is" with no warranties of any kind and may be subject to additional terms. Qlik reserves the right at any time, in its sole discretion, to discontinue provision of, or to modify, any such features or functionality provided for testing purposes.

9.4 **Third Party Materials**. Qlik Products may incorporate or otherwise access certain open source or other third-party software, data, services, or other materials for the hosting and delivery of the Qlik Products, which are identified in the Documentation (the "Third-Party Materials"). Qlik represents that if the Qlik Products are used in accordance with this Agreement, such use shall not violate any license terms for the Third-Party Materials. Qlik makes no other representation, warranty, or other commitment regarding the Third-Party Materials, and hereby disclaims any and all liability relating to Customer's use thereof.

9.5 **Connectivity to Third-Party Applications**. Use of Qlik Products to connect or interoperate with or access third-party web-based applications or services may be governed by terms and conditions established by such third party. Third-party application programming interfaces and other third-party applications or services ("Third-Party Applications") are not managed by Qlik, and Qlik shall have no liability for connectivity if any Third-Party Applications are changed or discontinued by the respective third parties. Qlik does not support, license, control, endorse or otherwise make any representations or warranties regarding any Third-Party Applications.

9.6 **Force Majeure**. FAR 52.212-4(f) governs all excusable delays defined as an occurrence beyond the reasonable control of the Qlik and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. Qlik will notify the Customer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Customer of the cessation of such occurrence.

9.7 **Recordkeeping, Verification and Audit**. While this Agreement is in effect and for one (1) year after the effective date of its termination, upon request by Qlik but not more than once per calendar year, Customer shall conduct a self-audit of its use of the Qlik Products and, within ten (10) business days after receipt of such request, submit a written statement to Qlik verifying that it is in compliance with the terms and conditions of this Agreement. Qlik shall have the right, on its own or through its designated agent or third-party accounting firm, to conduct an audit of Customer's use and deployment of the Qlik Products and monitor use of Qlik Cloud Government, in order to verify compliance with this Agreement. Qlik's written request for audit will be submitted to Customer at least fifteen (15) days prior to the specified audit date, and such audit shall be conducted during regular business hours and with the goal of minimizing the disruption to Customer's business. If such audit discloses that Customer is not in material compliance with the terms of this Agreement, then Customer shall be responsible for the reasonable costs of the audit, in addition to any other fees or damages to which Qlik may be entitled under this Agreement and applicable law.

9.8 **Commercial Terms**. Qlik Cloud Government is a commercial item and commercial off the shelf product as defined in FAR Part 202-1. These Terms reflect (a) standard commercial practices for the acquisition of Qlik Cloud Government and (b) terms and conditions that Qlik customarily provides to its other customers. These Terms apply to the Customer's use of Qlik Cloud Government as consistent with applicable law and regulation. If the Agreement conflicts with applicable law and regulation (such as FAR Part 12.212(a)), those terms are deleted and unenforceable as applied to any Order Forms. Qlik developed Qlik Cloud Government solely at private expense. All other use is prohibited.

9.9 **Assignment; Relationship between the Parties.** Unless law or regulation prohibit restrictions on transfer, Customer may only assign the Terms, any Order Form, or any right or obligation under the Agreement, or delegate any performance, with Qlik's prior written consent, which will not be unreasonably withheld. Qlik may assign its right to receive payment in accordance with the Assignment of Claims Act (31 U.S.C. § 3727) and FAR 52.212-4(b), and may assign the Agreement if the Anti-Assignment Act (41 U.S.C. § 15) does not prohibit the transfer. Subject to FAR 42.12 (Novation and Change-of-Name Agreements), Customer must recognize Qlik's successor in interest following a transfer of all or substantially all of Qlik's assets or a change in Qlik's name. Any assignment contrary to this Section will be void. The Agreement will be binding upon and benefit the parties and their respective successors and assigns. No agency, partnership, joint venture, fiduciary, or employment relationship is created as a result of this Agreement and neither party has any authority of any kind to bind the other in any respect.

9.10 **Notices.** All notices concerning a default, breach or violation of this Agreement by Qlik must be in writing and delivered to Qlik: (a) by certified or registered mail; or (b) by an internationally recognized express courier, and shall be addressed to: Qlik at 211 S. Gulph Rd., Suite 500, King of Prussia, PA 19406 USA, Attention: Legal Department. All other notices to Qlik, including account related communications, will be electronically sent to Qlik at CustomerNotices@qlik.com. Unless otherwise specified in writing by the Customer, all notices to Customer shall be sent to the address provided by Customer in the Order Form.

9.11 .

9.12 **Evaluation Subscriptions**. (a) Qlik may make a free evaluation subscription of Qlik Products ("Free Evaluation Subscription:") If Customer uses a Free Evaluation Subscription, Qlik will make such Free Evaluation Subscription available to Customer on a trial basis, free of charge, until the earlier of (a) the end of the free trial period for such Free Evaluation Subscription, (b) the start date of Qlik Product subscription purchased by Customer for such or (c) termination of the Free Evaluation Subscription by Qlik in its sole discretion. Notwithstanding anything to the contrary in this Agreement, a Free Evaluation Subscription is provided "AS IS." QLIK MAKES NO REPRESENTATION OR WARRANTY AND SHALL HAVE NO INDEMNIFICATION OBLIGATIONS WITH RESPECT TO AN EVALUATION SUBSCRIPTION. QLIK SHALL HAVE NO LIABILITY OF ANY TYPE WITH RESPECT TO AN EVALUATION SUBSCRIPTION, UNLESS SUCH EXCLUSION OF LIABILITY IS NOT ENFORCABLE UNDER APPLICABLE LAW IN WHICH CASE QLIK'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO AN EVALUATION SUBSCRIPTION IS US$1,000. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN SECTION 5.4 ("LIMITATION OF LIABILITY"), CUSTOMER SHALL NOT USE THE AN EVALUATION SUBSCRIPTION IN A MANNER THAT VIOLATES APPLICABLE LAWS AND WILL BE FULLY LIABLE FOR ANY DAMAGES CAUSED BY ITS USE OF AN EVALUATION SUBSCRIPTION. ANY DATA AND CONFIGURATIONS ENTERED INTO CUSTOMER'S EVALUATION SUBSCRIPTION ACCOUNT MAY BE PERMANENTLY LOST UPON TERMINATION OF AN EVALUATION SUBSCRIPTION. (b) For Government Users: Qlik may provide a free Evaluation Subscription to the Qlik Products and Documentation to the U.S. Government as "commercial items," "commercial computer software," "commercial computer software documentation," and "technical data". If Customer or any Authorized User is using the Evaluation Subscription on behalf of the U.S. Government and these terms fail to meet the U.S.

Government's needs or are inconsistent in any respect with federal law, Customer and Customer's Authorized Users must immediately discontinue use of the evaluation. The terms listed above are defined in the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement

## Table 1
## Governing Law and Venue

| Customer Location | Qlik Contracting Entity | Governing Law |
|---|---|---|
| United States, Puerto Rico, Jamaica, Virgin Islands (US) or Haiti | QlikTech Inc. | (i) Federal laws of the United States govern the Agreement without reference to conflict of laws. In the absence of federal laws and/or to the extent federal law permits, the Governing Law shall be the laws of the Commonwealth of Pennsylvania, USA excluding the conflict of law principles, and<br>(ii) any suit, action or proceeding arising out of or relating to this Agreement (including any non-contractual dispute or claim) will be settled by the State and Federal Courts of Montgomery County in the Commonwealth of Pennsylvania. |

# Qlik Cloud Government Service Level Agreement

This Qlik Cloud Government Service Level Agreement ("Policy") describes the current practices of Qlik with regard to its provision of Support Services as defined below to customers with a Qlik Cloud Government subscription ("Customer(s)").

## 1. Definitions

**"Affiliate"** means any entity which controls, is controlled by, or is under common control with Customer where "control" means the legal, beneficial or equitable ownership of at least a majority of the aggregate of all voting equity interests of such entity, but only for so long as such control exists.

"**Agreement**" means the written agreement between Qlik and Customer for Qlik Cloud Government.

**"Authorized Affiliate"** means any Affiliate of Customer that is designated by Customer as authorized to use a Qlik Cloud Government subscription if permitted under the terms of an Agreement.

**"Documentation"** means the then-current user documentation for Qlik Cloud Government, including any product metrics available at www.qlik.com/product-terms, as may be modified by Qlik from time to time.

**"Error"** means any verifiable and reproducible failure of Qlik Cloud Government to materially conform to the Documentation.

**"Initial Response Time"** means the period commencing when an Error is first reported by Customer's Technical Contact(s) in the manner required by this Policy and ending when a member of the Qlik technical support team logs the report and responds to the Technical Contact(s) in accordance with this Policy..

**"Qlik Cloud Government"** refers to any paid SaaS offering deployed on Qlik's Government Cloud.

"**Self-Service Tools**" means the Knowledge Base (Qlik's online database of content and FAQs), white papers, Community Forums, webcasts and other materials available in the Support Portal to Customers.

**"Severity 1 Error"** means that Qlik Cloud Government is down or not available due to (i) a server-side failure, but not as a result of scheduled maintenance and/or upgrades, or (ii) any event beyond the reasonable control of Qlik, including but not limited to any interruption of power, third party hosting companies, telecommunications and/or Internet connectivity, and any failure of Customer's internal telecommunications equipment, browser or network configurations, hardware and/or third party software).

**"Severity 2 Error"** means that major functionality is materially impacted and not working in accordance with the technical specifications in the Documentation or significant performance degradation is experienced so that critical business operations cannot be performed.

**"Severity 3 Error"** means any Error that is not a Severity 1 Error or Severity 2 Error.

"**Standard Business Hours**" mean from 08:00 to 17:00 ET (8:00 am to 5:00 pm), Monday to Friday (excluding national and bank holidays).

"**Support Portal**" means Qlik's online support website available at https://community.qlik.com/t5/Support/ct-p/qlik.

**"Support Services"** means the technical end user support for Qlik Cloud Government as described in this Policy. Support Services do not include services performed onsite at any Customer facility, consulting or education services or any services not expressly stated in this Policy.

**"Technical Contact(s)"** means Customer's personnel that have been identified in writing by Customer as the technical contact(s) for Customer and authorized to contact Qlik for support.

"**Update**" means a subsequent release of Qlik Cloud Government which Qlik generally makes available at no additional fee.

## 2. Overview

2.1 Qlik will provide Customer with Support Services for Qlik Cloud Government in accordance with this Policy, subject to Customer's timely payment of the applicable subscription fees. Support Services provided by Qlik hereunder will be provided in the English language

2.2 Unless otherwise expressly set forth herein, all references in this Policy to response times or communications from Qlik shall only apply during Qlik's Standard Business Hours, regardless of when a support matter is reported to Qlik.

## 3. Support Levels

3.1 Enterprise Support Coverage for Qlik Cloud Government .

3.1.1. Qlik will use commercially reasonable efforts to respond within the applicable initial response time targets set forth in the tables below for Severity 1, 2 and 3 Errors in Qlik Cloud Government reported by a Technical Contact to Qlik via email at government.support@qlikcloudgov.com. Qlik will respond to Customer's Technical Contact by telephone or email. All Errors will be initially logged and acknowledged by Qlik during Qlik's Standard Business Hours.

**Support Coverage for Qlik Cloud Government**

| Severity Level | Initial Response Time | Communication Frequency |
|---|---|---|
| Severity 1 Error | 30 minutes* | Every 4 hours* |
| Severity 2 Error | 1 hour* | 48 Hours* |
| Severity 3 Error | 4 hours* | Weekly* |

*During Standard Business Hours

3.1.2 Qlik will report known outages of Qlik Cloud Government on Qlik's status page, currently located at status.qlikcloud.com ("Status Page"). If a suspected outage is not listed on the Status Page, Customer may contact Qlik to report the suspected outage via email to government.support@qlikcloudgov.com. Qlik will respond to such report via email, by posting an update on the Status Page or by telephone. Scheduled maintenance times for Qlik Cloud Government will be posted on the Support Portal. Qlik endeavors to provide at least forty-eight (48) hours prior posting of any scheduled maintenance for the Qlik Cloud Government.

3.2 Updates. Updates for Qlik Cloud Government automatically replace the previous version of the Qlik Cloud Government. Updates do not include new or separate products which Qlik offers only for an additional fee to its customers generally.

## 4. Error Resolution and Escalation

4.1 An Error is considered to be resolved upon the earlier to occur of the following: (i) Qlik and Customer mutually agree in writing that the issue or problem is resolved; (ii) Qlik has provided an Update; (iii) a technical work-around solution is provided and is reasonable in Qlik's discretion; (iv) Customer requests that Qlik close the support case; or (v) the support case has been left open by the Customer for ten (10) consecutive business days, during which period Qlik has not received a response from any of Customer's Technical Contacts.

4.2 Exclusions. Notwithstanding anything in this Policy to the contrary, Qlik will have no obligation to provide any Support Services in connection with: (i) any issue or problem that Qlik determines is not due to any Error or deficiency in Qlik Cloud Government (including without limitation, issues or problems caused by stand-alone third party software products used in conjunction with Qlik Cloud Government, the Internet or other communications, Customer network or browser matters, or login issues); (ii) use of Qlik Cloud Government other than in accordance with the Documentation and the Agreement; (iii) use of Qlik Cloud Government provided on a trial or evaluation basis or for which Customer has not paid any fees; (iv) any Errors or problems with the Qlik Cloud Government that are not reproducible; (v) any Error or problem that is not reported by Customer via email to government.support@qlikcloudgov.com; or (vi) any Error or problem that would require Qlik to have access to Customer's Qlik Cloud Government tenant in order to provide Support Services. If Qlik does correct any of the Errors described in subsections (i)-(v) above, or otherwise provides support for Qlik Cloud Government that is not covered by the terms and conditions contained in this Policy, such Error resolution or support will be provided only following Customer's written request and approval of all charges, and Customer will be invoiced for such support at Qlik's then-current "time and materials" rates for such services. Without limiting any of the foregoing, Qlik has no obligation to provide support for any third party software, data, or other materials distributed or bundled with Qlik Cloud Government.

## 5. Customer's Obligations

5.1 Customer will provide timely information and access to knowledgeable resources as reasonably required to provide Support Services. Qlik's support obligations shall be excused to the extent Customer fails to cooperate in this regard.

5.2 The Customer shall: (i) not request, permit or authorize anyone other than Qlik (or a Qlik-authorized partner or provider) to provide any form of support services in respect of Qlik Cloud Government; (ii) cooperate fully with Qlik's personnel in the diagnosis or investigation of any Error or other issue or problem with Qlik Cloud Government; (iii) be responsible for maintaining all third party software not explicitly licensed under the Agreement; and (iv) be fully responsible for the actions of any third party (including any Qlik-authorized partner or provider) that it allows to access any information relating to Support Services.

5.3 Customer's contact with Qlik in connection with Customer's requests for support and reports of Errors shall be solely through its Technical Contact(s). The Technical Contact(s) shall: (i) serve as the internal contact(s) for Customer's and its Authorized Affiliates' personnel who are authorized to use Qlik Cloud Government per the terms of the Agreement; (ii) be responsible for initiating all requests by, and maintaining all records of, the Customer and its Authorized Affiliates relating to Support Services; (iii) serve as the contact(s) with Qlik on all matters relating to Support Services; and (iv) be responsible for providing information and support, as requested by Qlik, to assist in the reproduction, diagnosis, analysis, and resolution of Errors. The maximum number of Technical Contacts for each Customer is six (6), regardless of the number or types or quantities of subscriptions purchased by the Customer. Customer shall ensure that its Technical Contacts comply with any reasonable training requirements for the Technical Contact(s) upon notification by Qlik. Subject to the previous sentence, Customer may change its Technical Contact(s) by notifying Qlik in writing.

5.4 Customer will be responsible for primary support of any Authorized Affiliates in connection with their use of Qlik Cloud Government in accordance with the terms of the Agreement. Customer is solely responsible for: (i) passing on to its Authorized Affiliates all support materials as appropriate; and (ii) providing software support, including operational instruction, problem reporting and technical advice to its Authorized Affiliates, as necessary to enable the Authorized Affiliate to continue to use Qlik Cloud Government as authorized under the Agreement. Customer's Authorized Affiliates, as well as its contractors and third party users, may not contact Qlik directly for support, unless designated as a Technical Contact by the Customer.

5.5 For certain services provided under this Policy, the transmission of machine logs and/or sharing of data via screen share may be required. For avoidance of doubt, Customer shall not include any business sensitive and/or personal information via transmissions relating to Support Services. Customer shall take reasonable measures to anonymize such data before providing the data to Qlik. However, should Qlik agree to accept any log files or other information containing personal data, Qlik will comply with Qlik's privacy policies, available to view online at www.qlik.com.

## 6. Additional Terms

6.1 Open Source. Qlik may make certain open source libraries available for use with Qlik Cloud Government as described in the Documentation ("Qlik Libraries"). Qlik Libraries identified at https://qlik.dev/support are eligible for support, provided that Qlik shall only be obligated to support: (i) the most current release, (ii) Qlik Libraries which have not been changed, modified or altered in any manner except by Qlik, and (iii) Qlik Libraries used in accordance with the Documentation. Any other open source software leveraging and extending Qlik Cloud Government (an "Extension") and released by Qlik on various online communities is supported solely by the open source community. Extensions, which are developed by Qlik's partners, including certified Extensions, are also not eligible for support under this Policy

6.2 Qlik may elect to make certain software available free of charge for trial, evaluation or other purposes ("Freeware"). Support for Freeware, if any, will be provided at Qlik's discretion and in accordance with the license terms for such Freeware.

6.3 Support for QSE Client Managed for QSE SaaS – Government (US). If Customer has licensed QSE Client Managed for QSE SaaS – Government US) Licenses in connection with its use of Qlik Cloud Government, the provisions of Sections 2 through 5, inclusive, of this Policy shall apply to such product.

## 7. Changes to Policy

Subject to the terms of the Agreement, Qlik reserves the right, at its discretion, to non-materially change the Policy at any time based on prevailing market practices and the evolution of Qlik's products and services.

## 8. Disclaimer

THIS POLICY DEFINES A SERVICE ARRANGEMENT AND NOT A WARRANTY. QLIK CLOUD GOVERNMENT IS SUBJECT EXCLUSIVELY TO THE WARRANTIES SET FORTH IN THE APPLICABLE AGREEMENT. THIS POLICY DOES NOT CHANGE OR SUPERSEDE ANY TERM OF ANY SUCH AGREEMENT. TO THE EXTENT THERE IS A CONFLICT BETWEEN A TRANSLATED VERSION OF THIS POLICY AND THIS ENGLISH VERSION, THE ENGLISH LANGUAGE VERSION WILL PREVAIL.

# QLIK® DATA PROCESSING ADDENDUM

This Data Processing Addendum including its Schedules 1, 2, 3 and 4 (the "**DPA**"), once executed and received by Qlik according to the instructions below, forms part of the Agreement between Qlik and the Customer (each defined below).

The Qlik party to this DPA is the Qlik entity that is the Qlik party to the Agreement. Only the Customer entity that is the party to the Agreement may sign this DPA. If the Customer entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA. The Customer's signatory represents and warrants that he or she has the legal authority to bind the Customer to this DPA.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

In order for it to be effective, the Parties must (a) complete and sign the information block below with the Customer full legal entity details and signatory information and (b) sign Schedule 4 (2021 SCCs).

The Parties hereby agree from the Effective Date to be bound by the terms and conditions of this DPA.

| **Accepted and agreed to by Qlik** | | **Accepted and agreed to by the Customer** | |
|---|---|---|---|
| *Name of signatory* | Roy Horgan | *Customer legal name (include entity type, e.g., Inc., Ltd., etc.)* | |
| | | *Country of customer* | |
| *Position* | Senior Director, Privacy Counsel and Data Protection Officer | *Name of signatory* | |
| *Signature* | | *Position* | |
| *Date* | | *Signature* | |
| | | *Date* | |
| *Key privacy contact* | Roy Horgan, Senior Director, Privacy Counsel and Data Protection Officer<br>privacy@qlik.com | *Key privacy contact* | |

# SCHEDULE 1
# DATA PROTECTION OBLIGATIONS

This DPA is an agreement between the Customer and Qlik governing the Processing by Qlik of Customer Personal Data in its performance of the Services. Capitalized terms used in the DPA will have the meanings given to them in Section 1 below.

## 1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Agreement**" means either (i) the Qlik Customer Agreement or (ii) the Qlik OEM Partner Agreement, between Qlik and the Customer under which Qlik provides the applicable Services.

"**CCPA**" means the California Consumer Privacy Act, as amended, and its implementing regulations. The terms "**Business**" and "**Service Provider**" where used in this DPA addressing compliance under the CCPA will have the meanings given to them under the CCPA.

"**Client-Managed Deployment**" means a deployment of on-premise Qlik or Qlik Affiliate software managed and/or hosted by the Customer or by a Customer's third party cloud provider.

"**Consulting Services**" means any consulting services provided to the Customer by Qlik pursuant to the Agreement.

"**Customer**" means the customer legal entity which is a Party to the Agreement.

"**Customer Personal Data**" means Personal Data which Qlik Processes on behalf of the Customer in the performance of the Services, including, where applicable, Cloud Customer Content. It does not include Personal Data for which Qlik is a Controller.

"**Data Protection Law**" means, as amended from time to time, the Australia Privacy Act, the Brazil General Data Protection Law (LGPD), the Canada Personal Information Protection and Electronic Documents Act, the EU GDPR, the Israel Protection of Privacy Law, the Japan Act on the Protection of Personal Information, the Singapore Personal Data Protection Act, Swiss Federal Act on Data Protection, the UK Data Protection Act 2018 and UK General Data Protection Regulation, and the general consumer (non-industry specific) data privacy laws of the United States and its states (including, where applicable, the CCPA), and in each case only to the extent applicable to the performance of either Party's obligations under this DPA.

"**DPF**" means the EU-U.S. Data Privacy Framework, including the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework.

"**Effective Date**" means the date on which Qlik receives a validly executed DPA under the instructions above and always subject to the Customer having validly executed an Agreement.

"**EEA**" means, for the purpose of this DPA, the European Economic Area (including the European Union) and, for the purposes of this DPA, Switzerland.

"**EEA Customer Personal Data**" means Customer Personal Data that is subject to the EU GDPR.

"**EU GDPR**" means, in each case to the extent applicable to the Processing activities (i) Regulation (EU) 2016/679; and (ii) Regulation (EU) 2016/679 as amended by any legislation arising out of the withdrawal of the UK from the European Union.

"**Party**" or "**Parties**" means Qlik and the Customer, individually and collectively, as the case may be.

"**Personal Data**" means information relating to an identified or identifiable natural person or as otherwise defined under applicable Data Protection Law.

"**Personnel"** means a Party's employees or other workers under their direct control.

"**Qlik**" means the Qlik Affiliate which is party to the Agreement.

"**Qlik Cloud Customer Content**" means information, data, materials, media, or other content to the extent it includes Customer Personal Data that is, by, on behalf of or upon the instructions of the Customer, uploaded into and residing in Qlik Cloud which Qlik or a Qlik Affiliate Processes on behalf of the Customer.

"**Qlik Cloud**" means a subscription-based, hosted solution provided and managed by Qlik or an Affiliate under an Agreement.

"**Qlik DPF Companies**" means the U.S. Affiliates of the Group which participate in the DPF, found at https://www.dataprivacyframework.gov/s/.

"**Security Incident**" means unauthorized or unlawful destruction, loss, alteration or access to, or disclosure of, Customer Personal Data that is in Qlik's possession or under Qlik's control in its performance of the Services. It does not include events which are either (i) caused by the Customer or Customer Affiliates or their end users or third parties operating under their direction, such as the Customer's or Customer Affiliate's failure to (a) control user access; (b) secure or encrypt Customer Personal Data which the Customer transmits to and from Qlik during performance of the Services; and/or (c) implement security configurations to protect Customer Personal Data; or (ii) unsuccessful attempts or activities that do not or are not reasonably likely to compromise the security of Customer Personal Data, including but not limited to unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Service(s)**" means, pursuant to an Agreement, (i) Qlik Cloud, (ii) a Qlik Cloud trial, (iii) a Qlik Cloud presales proof-of-concept performed by Qlik, and/or (iv) Support Services and/or Consulting Services requiring Qlik personnel to access or otherwise Process on Customer's behalf either (a) Qlik Cloud Customer Content while within or originating from Qlik Cloud and/or (b) Customer Personal Data relating to a Client-Managed Deployment, and in each case, only as it relates to Processing by Qlik or a Qlik Affiliate of Customer Personal Data. Notwithstanding the foregoing, "Services" does not include, and accordingly, this DPA does not cover, (i) Qlik Cloud Customer Content which leaves Qlik Cloud, and/or (ii) Customer Personal Data stored in a Client-Managed Deployment, including but not limited to Customer Personal Data stored within self-hosted software.

"**Support Services**" means end user support provided by Qlik or an Affiliate to the Customer under the Agreement involving Processing by Qlik of Customer Personal Data either by way of (i) temporary remote access or screenshare, and/or (ii) receipt by Qlik or a Qlik Affiliate of Customer files via Qlik's support portal.

"**Swiss Customer Personal Data**" means Customer Personal Data that is subject to the Swiss Federal Act on Data Protection.

"**Termination Date**" means the termination or expiration of the relevant Service(s) under the Agreement between the Parties, or, in the case of a Qlik Cloud presales proof-of-concept or trial, the termination or expiration of that presales proof-of-concept or trial.

"**Third Country**" means a third country not deemed by the EU Commission, Swiss Federal Council or UK Information Commissioner, as applicable, to have an equivalent level of privacy protection to those jurisdictions.

"**UK Addendum**" means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner and laid before Parliament in accordance with S119A(1) Data Protection Act 2018 on 2 February 2022 but, as permitted by Section 17 of such Addendum, the format of the information set out in Part 1 of the Addendum shall be amended as set out in Section 5.4 of this DPA.

"**UK Customer Personal Data**" means Customer Personal Data that is subject to the UK General Data Protection Regulation.

"**2021 SCCs**" means the 2021 SCCs Module Two and the 2021 SCCs Module Three, collectively or individually, as applicable, published under EU Commission Decision 2021/914/EU for EU Personal Data transfers outside the EU to Third Countries not deemed by the EU Commission to have an equivalent level of privacy protection, included as Schedule 4. The terms "**2021 SCCs Module Two**" means the 2021 SCCs, module two (controller to processor), and "**2021 SCCs Module Three**" means the 2021 SCCs, module three (processor to processor).

"**Controller**", "**Data Subject**", "**Processor**", "**Process/Processed/Processing**", "**Subprocessor**" and "**Supervisory Authority**", and analogous terms, will be interpreted in accordance with Data Protection Law.

## 2. PROCESSING BY QLIK OF CUSTOMER PERSONAL DATA

**2.1 Details of Processing.** The table below in this Section 2.1 sets out the Customer Personal Data Qlik may Process when providing the Services:

| | |
|---|---|
| **Nature/Activities/Purpose of Processing** | Processing of Customer Personal Data by the Customer in Qlik Cloud and/or for Support or Consulting Services. |
| **Frequency and Duration of Processing** | From time to time during the term of the Services under the Agreement or, in the case of a Qlik Cloud presales proof-of-concept or trial, the term of that proof-of-concept or trial. Duration of Processing and retention period shall be the duration of the Services unless Customer Personal Data is deleted sooner. |
| **Types of Personal Data Processed** | Customer Personal Data uploaded to and residing in Qlik Cloud and/or otherwise Processed by Qlik to provide the Services. Customer Personal Data may include sensitive Personal Data if provided by the Customer. |
| **Categories of Data Subjects whose Personal Data is Processed** | Qlik will not be aware of what Personal Data the Customer may provide for the Services. It is anticipated that Data Subjects may include employees, customers, prospects, business partners and vendors of the Customer. |

**2.2 Purpose of Processing Customer Personal Data.** The Parties agree that either (a) the Customer is the Controller and Qlik is a Processor, or (b) Customer is the Processor and Qlik is a Subprocessor, in relation to the Customer Personal Data that Qlik Processes on the Customer's behalf in the course of providing the Services. For the avoidance of doubt, this DPA does not apply to Personal Data for which Qlik is a Controller. Qlik will Process Customer Personal Data only to perform the Services and for no other purpose. If Qlik is required to Process the Customer Personal Data for any other purpose by applicable laws to which Qlik is subject, Qlik will, unless prohibited by such applicable laws and subject to the terms of this DPA, inform Customer of this requirement first. To the extent that the CCPA applies to the Processing of Customer Personal Data in the course of providing the Services, (i) Qlik is a Service Provider and the Customer is a Business in relation to Customer Personal Data, and (ii) without limiting any other term in this DPA or in the Agreement, Qlik shall not (a) sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic means, any Customer Personal Data to any third-party for monetary or other valuable consideration, (b) retain, disclose, or use any Customer Personal Data for any purpose (including any commercial purpose) other than the specific purpose of performing the Services, and/or (c) retain, use, or disclose any Customer Personal Data outside of the direct business relationship between the Customer and Qlik. Qlik hereby certifies that it understands the restrictions described in the previous sentence and shall comply with them. To the extent that any database registration requirements are required under local laws a result of Customer's use of the Services, Customer warrants that it shall undertake any such legally required registrations.

**2.3 Disclosure of Customer Personal Data.** Unless otherwise provided for in this DPA, Qlik will not disclose to any third party any Customer Personal Data, except, in each case, as necessary to maintain or provide the Services, or, notwithstanding Section 5.7 below, as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order).

**2.4 Customer Personal Data for Support Services.** The Parties acknowledge that Qlik does not ordinarily require to Process Customer Personal Data on the Customer's behalf to resolve a technical issue for Support Services. Accordingly;

2.4.1 the Customer shall use their best efforts to minimize any transfer of Customer Personal Data to Qlik for Support Services. Such efforts shall include but not be limited to removing, anonymizing and/or pseudononymizing Customer Personal Data in files prior to Processing by Qlik; and

2.4.2 Qlik's total liability in relation to the Processing of Support Services Customer Personal Data, whether in contract, tort or under any other theory of liability, shall not exceed US$20,000.

**2.5 Obligations of Qlik Personnel.** Qlik will ensure that Qlik Personnel required to access the Customer Personal Data are subject to a binding duty of confidentiality in respect of such Customer Personal Data and take reasonable steps to ensure the reliability and competence of such Qlik Personnel.

**2.6 Instructions.** Customer authorizes and instructs Qlik to Process Customer Personal Data for the performance of the Services. The Parties agree that this DPA and the Agreement are the Customer's complete and final documented Processing instructions to Qlik in relation to Customer Personal Data. The Customer shall ensure that its Processing instructions comply with applicable Data Protection Laws in relation to Customer Personal Data and that the Processing of Customer Personal Data in accordance with the Customer's instructions will not cause Qlik to be in breach of any relevant law. The Customer warrants that it has the right and authority under applicable Data Protection Law and any undertakings it may have entered into to disclose, or have disclosed, Customer Personal Data to Qlik to be Processed by Qlik for the Services and that the Customer has obtained all necessary consents and provided all necessary notifications required by Data Protection Law with respect to the Processing of Customer Personal Data by Qlik. The Customer will not disclose Customer Personal Data to Qlik or instruct Qlik to Process Customer Personal Data for any purpose not permitted by applicable law, including Data Protection Law. Qlik will notify the Customer if Qlik becomes aware that, and in Qlik's reasonable opinion, an instruction for the Processing of Customer Personal Data given by the Customer violates Data Protection Law, it being acknowledged that Qlik is not under any obligation to undertake additional work, screening or legal assessment to determine whether Customer's instructions are compliant with Data Protection Law.

**2.7 Assistance to the Customer.** Upon a written request, Qlik will provide reasonable cooperation and assistance necessary to assist the Customer, insofar as required by Data Protection Law and as it relates to Processing by Qlik for the Services, in fulfilling the Customer's obligations to respond to requests from Data Subjects exercising their rights (notwithstanding the Customer's obligations in Section 7) and/or to carry out data protection impact assessments. Qlik's Data Protection Officer and privacy team may be reached at privacy@qlik.com.

**2.8 Compliance with Data Protection Laws.** Each Party will comply with the Data Protection Laws applicable to it in relation to their performance of this DPA, including, where applicable, the EU GDPR.

## 3. SECURITY

**3.1 Security of Data Processing.** Qlik will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data against unauthorized or unlawful Processing and against Security Incidents. These measures will be appropriate to the harm, which might result from any unauthorized or unlawful Processing, accidental loss, destruction, damage or theft of the Customer Personal Data and having regard to the nature of the Customer Personal Data which is to be protected. At a minimum, these will include the measures set out in Schedule 2.

**3.2 Notification of a Security Incident.** Upon becoming aware of a Security Incident, Qlik or a Qlik Affiliate will notify the Customer without undue delay and take reasonable steps to identify, prevent and mitigate the effects of the Security Incident and to remedy the Security Incident to the extent such remediation is within Qlik's reasonable control. A notification by Qlik or a Qlik Affiliate to the Customer of a Security Incident under this DPA is not and will not be construed as an acknowledgement by Qlik of any fault or liability of Qlik with respect to the Security Incident.

**3.3 Notification Mechanism.** Security Incident notifications, if any, will be delivered to Customer by any means Qlik selects, including via email. It is the Customer's responsibility to ensure that it provides Qlik with accurate contact information and secure transmission at all times.

## 4. SUBPROCESSORS

**4.1 Authorized Subprocessors.** The Customer agrees that Qlik may use its Affiliates and other Subprocessors to fulfil its contractual obligations under this DPA or to provide certain Services on its behalf. The Qlik website lists Subprocessors that are currently engaged by Qlik to carry out Processing activities on Customer Personal Data (currently located at https://community.qlik.com/t5/Qlik-Technical-Bulletin-Blog/Qlik-Subprocessors-General-Data-Protection-Regulation-GDPR/ba-p/1572352). The Customer may subscribe to the list in order to receive Subprocessor updates.

**4.2 Subprocessor Obligations.** Where Qlik uses a Subprocessor as set forth in this Section 4, Qlik will (i) enter into a written agreement with the Subprocessor and will impose on the Subprocessor contractual obligations not less protective on an aggregate basis than the overall obligations that Qlik has provided under this DPA, including but not limited to, where applicable, incorporating the 2021 SCCs and/or the UK Addendum; and (ii) restrict the Subprocessor's access to and use of Customer Personal Data only to provide the Services. For the avoidance of doubt, where a Subprocessor fails to fulfil its obligations under any subprocessing agreement or any applicable Data Protection Law with respect to Customer Personal Data, Qlik will remain liable, subject to the terms of this DPA, to the Customer for the fulfilment of Qlik's obligations under this DPA.

**4.3 Appointing a New Subprocessor.** At least thirty (30) days before Qlik engages any new Subprocessor to carry out Processing activities on Customer Personal Data, Qlik will provide notice of such update to the Subprocessor list through the applicable website. If the Customer is entitled to do so under applicable Data Protection Law and as it relates to the Processing of Customer Personal Data by the Subprocessor, the Customer may make reasonable objections in writing to privacy@qlik.com within the 30-day period regarding the appointment of the new Subprocessor. After receiving such written objection Qlik will either: (i) work with the Customer to address the Customer's objections to its reasonable satisfaction, (ii) instruct the Subprocessor not to Process Customer Personal Data, provided that the Customer accepts that this may impair the Services (for which Qlik shall bear no responsibility or liability), or (iii) notify the Customer of an option to terminate this DPA and the applicable order form for Services which cannot be provided by Qlik without the use of the objected-to new subprocessor. If Qlik does not receive an objection from the Customer within the 30-day objection period, the Customer will be deemed to have consented to the appointment of the new Subprocessor.

## 5. EEA/UK THIRD COUNTRY DATA TRANSFERS

**5.1 Transfers of EEA Customer Personal Data.** For transfers of EEA Customer Personal Data by the Customer to Qlik, where the Qlik party to this DPA is in a Third Country not deemed under EEA Data Protection Law to provide an equivalent level of privacy protection to that in the EEA and is not one of the Qlik DPF Companies;

5.1.1 where the Customer is the Controller and Qlik a Processor of such EEA Customer Personal Data, such transfer(s) are subject to the 2021 SCCs Module Two; and/or

5.1.2 where the Customer is the Processor and Qlik a Subprocessor of such EEA Customer Personal Data (i.e., where the EEA Customer Personal Data contains EEA Personal Data of the Customer's customers where the Customer is a Processor), such transfer(s) are subject to the 2021 SCCs Module Three;

in each case, the 2021 SCCs Module Two and 2021 SCCs Module Three, as applicable, shall apply as set out in Schedule 4 and subject to the provisions of this DPA.

**5.2 Particulars regarding the 2021 SCCs.** The 2021 SCCs are particularized in Schedule 4. The Parties agree that, to the fullest extent permitted under the 2021 SCCs, (a) the aggregate liability of Qlik to the Customer under or in connection with the 2021 SCCs will be limited as set out in sections 2.4 and 8.3 of this DPA, and (b) any rights to audit pursuant to Clause 8.9 of the 2021 SCCs will be exercised in accordance with section 6 below.

**5.3 Swiss Customer Personal Data.** For transfers of Swiss Customer Personal Data by the Customer to Qlik where the Qlik party to this DPA is in a Third Country not deemed under the Swiss Data Protection Law to provide an equivalent level of privacy protection to that in Switzerland and the Qlik party is not one of the Qlik DPF Companies, the Parties agree that the 2021 SCCs shall apply as set out in Schedule 4 and as particularized in clauses 5.1 and 5.2 of this DPA, save that references (i) to the EU GDPR shall be replaced by the respective references and/or equivalent terms in the Swiss Federal Act on Data Protection, (ii) to the competent supervisory authority in Annex I. C. shall be replaced with the Swiss Federal Data Protection and Information Commissioner, and (iii) to Member State(s), the EU and the EEA shall include Switzerland.

**5.4 UK Customer Personal Data**. For transfers of UK Customer Personal Data by the Customer to Qlik where the Qlik party to this DPA is in a Third Country not deemed under UK Data Protection Law to provide an equivalent level of privacy protection to that in the UK and the Qlik party is not one of the Qlik DPF Companies, the Parties agree that the provisions of the UK Addendum shall apply to such transfers. In particular:

5.4.1 the Customer will be the data exporter, and Qlik the data importer;

5.4.2 the start date for transfers in Table 1 of the UK Addendum shall be the Effective Date unless otherwise agreed between the Parties;

5.4.3 the details of the Parties and their key contacts in Table 1 of the UK Addendum shall be as set out at the commencement of this DPA, and with no requirement for additional signature;

5.4.4 for the purposes of Table 2, the UK Addendum shall be appended to the 2021 SCCs as incorporated by reference into this DPA (including the selection of modules as specified in Section 5.1, the particulars as specified in Section 5.2 of this DPA and the selection and disapplication of optional clauses as set out in Schedule 4);

5.4.5 the appendix information listed in Table 3 of the UK Addendum is set out at the commencement of this DPA (List of Parties), in Section 2 (Description of Transfer) and in Schedule 2 to this DPA (Technical and Organisational Measures); and

5.4.6 for the purposes of Table 4, neither Party may end the UK Addendum as set out in Section 19 thereof.

**5.5 Alternative Lawful Transfer Mechanisms.** The Customer acknowledges that Qlik's obligations under EEA/UK Third Country lawful transfer mechanisms (e.g. the 2021 SCCs, DPF) under this DPA may be replaced by obligations under any successor or alternate EEA/UK Third Country lawful transfer mechanism adopted by Qlik which is recognized by the relevant EEA/UK/Swiss authorities. In such instances, the Parties shall not be required to re-execute this DPA as they have already agreed to such measures, and such obligations will be deemed automatically included in this DPA. Customer acknowledges that, in the event of DPF no longer lawfully holding an adequacy decision, as judged by relevant EU/UK/Swiss authorities, a notification under section 5.6 (b) may be by way of an update by Qlik to its DPA terms at https://www.qlik.com/us/legal/legal-agreements.

**5.6 Transfers to Qlik DPF Companies.** If the Qlik party to this DPA is one of the Qlik DPF Companies, Qlik agrees to apply the DPF Principles issued by the U.S. Department of Commerce, located at https://dataprivacyframework.gov ("DPF Principles") to Customer Personal Data that Customer transfers to Qlik that originates from the European Economic Area, United Kingdom, or Switzerland if that Customer Personal Data meets the definition of "personal data" or "personal information" in the DPF Principles ("DPF Customer Personal Data"). For clarity, Qlik agrees to (a) use DPF Customer Personal Data only to provide the relevant Service; (b) notify the Customer if Qlik determines that it can no longer apply the DPF Principles to DPF Customer Personal Data; and (c) upon such determination, cease use of DPF Personal Data or take other reasonable and appropriate steps to apply the DPF Principles to DPF Customer Personal Data.

**5.7 EEA/UK-US Transfers.** In response to the Court of Justice of the European Union's decision in Schrems II, Case No. C-311/18, and related guidance from Supervisory Authorities, the Parties acknowledge that supplemental measures may be needed with respect to EEA/UK-U.S. data transfers where Customer Personal Data may be subject to government surveillance. The Customer and Qlik agree that Customer's EEA/UK operations involve ordinary commercial services, and any EEA/UK-U.S. transfers of EEA Customer Personal Data contemplated by this DPA involve ordinary commercial information, such as employee data, which is not the type of data that is of interest to, or generally subject to, surveillance by U.S. intelligence agencies. Accordingly, Qlik agrees that it will not provide access to Customer Personal Data of an EEA/UK Customer transferred under this DPA to any government or intelligence agency, except where its legal counsel has determined it is strictly relevant and necessary to comply with the law or a valid and binding order of a government authority (such as pursuant to a court order). If a law enforcement agency or other government authority provides Qlik with a demand for access to such Customer Personal Data, Qlik will attempt to redirect the law enforcement agency to request the Customer Personal Data directly from the Customer. If compelled by law to provide access to such Customer Personal Data to a law enforcement agency or other government authority, and only after a determination of such is made by legal counsel, then Qlik will, unless Qlik is legally prohibited from doing so: (1) give Customer notice of the demand no later than five (5) days after such demand is received to allow Customer to seek recourse or other appropriate remedy to adequately protect the privacy of EEA/UK Data Subjects, and Qlik shall provide reasonable cooperation in connection with the Customer seeking such recourse; and (2) in any event, provide access only to such Customer Personal Data as is strictly required by the relevant law or binding order (having used reasonable efforts to minimize and limit the scope of any such access). This Section 5.7 does not overwrite the equivalent protection under the relevant EEA/UK Third

Country lawful transfer mechanism (e.g., 2021 SCCs), if applicable.

**5.8 EEA Qlik Cloud Storage Capability.** For the avoidance of doubt, although the Customer may select (where available) the region in which its Qlik Cloud Customer Content resides, including the EU, the ability to retain Qlik Cloud Customer Content (including Customer Personal Data) solely in-region is subject to how the Customer's users of Qlik Cloud share and use applications and other technical particulars.

## 6. AUDITS

**6.1 Audit Reports.** Qlik and/or its relevant Affiliate(s) conduct periodic audits of its controls of relevant systems and processes (e.g., ISO 27001, SOC II), which may include systems and processes involved in the Processing of Customer Personal Data. These audits (i) occur on a regular, recurring basis, (ii) are performed according to the standards and rules of the relevant regulatory or accreditation body, (iii) are paid for by Qlik/its Affiliate(s), and (iv) produce an audit report ("Audit Report"). The Customer may request, and Qlik shall provide (subject to a NDA, where necessary), such Audit Report(s) or extracts thereof, where applicable to the Services, in order to satisfy the Customer of Qlik's compliance with statutory Processor obligations (e.g., Article 28 EU GDPR).

**6.2 Additional Information and Audits.** Where the information provided in the Audit Reports is not reasonably sufficient to demonstrate compliance by Qlik of its statutory Processor obligations in relation to the applicable Services, the Parties shall discuss in good faith any additional audits reasonably required by the Customer. Such additional audits, if agreed, must be (i) conducted by a third party agreed to by the Parties, (ii) carried out at the Customer's cost, (iii) be conducted in a manner undisruptive to the business of Qlik and its Affiliates, (iv) be conducted subject to the terms of an applicable non-disclosure agreement, and (v) not prejudice other confidential information (including but not limited to Personal Data) of Qlik, its Affiliates or its other customers.

**6.3 Subprocessor Audits.** If the Customer's request for information relates to a Subprocessor, or information held by a Subprocessor which Qlik cannot provide to the Customer itself, Qlik will promptly submit a request for additional information in writing to the relevant Subprocessor(s). The Customer acknowledges that information about the Subprocessor's previous independent audit reports is subject to agreement from the relevant Subprocessor, and that Qlik cannot guarantee access to that Subprocessor's audit information at any particular time, or at all.

## 7. ACCESS AND DELETION OF CUSTOMER PERSONAL DATA

**7.1 Access and Deletion of Qlik Cloud Customer Content during the Agreement.** Customer is responsible for any data minimization before inputting Customer Personal Data and for executing any requests to access, retrieve, correct and/or delete Qlik Cloud Customer Content (including any Customer Personal Data therein). Qlik will, as necessary to enable the Customer to meet its obligations under Data Protection Law, provide the Customer via availability of Qlik Cloud with the ability to access, retrieve, correct and delete through to the Termination Date its Qlik Cloud Customer Content in Qlik Cloud. The Customer acknowledges that such ability may from time to time be limited due to temporary service outage for maintenance or other updates to Qlik Cloud. To the extent that the Customer, in its fulfilment of its Data Protection Law obligations, is unable to access, retrieve, correct or delete Customer Personal Data in Qlik Cloud due to prolonged unavailability (for example, exceeding 10 working days) caused by an issue within Qlik's control, upon written request from the Customer, Qlik will where possible use reasonable efforts to provide, correct or delete such Customer Personal Data. The Customer acknowledges that Qlik may maintain backups of Qlik Cloud Customer Content, which would remain in place for approximately third (30) days following a deletion in Qlik Cloud. The Customer remains solely responsible for the deletion, correction and accuracy of its Qlik Cloud Customer Content and will be solely responsible for retrieving such Qlik Cloud Customer Content to respond to Data Subject access requests or similar requests relating to Customer Personal Data. If Qlik receives any such Data Subject request, Qlik will use commercially reasonable efforts to redirect the Data Subject to the Customer.

**7.2 Access and Deletion of Customer Personal Data on Termination of the Agreement**. By the Termination Date, the Customer will have deleted all Qlik Cloud Customer Content Personal Data, unless prohibited by law, or the order of a governmental or regulatory body. Notwithstanding the foregoing, after the Termination Date and upon the Customer's written request Qlik will provide reasonable assistance to the Customer to securely destroy or return any remaining Customer Personal Data. The Customer acknowledges that Customer Personal Data may be stored by Qlik after the Termination Date in line with Qlik's data retention rules and back-up procedures until it is eventually deleted. To the extent that any portion of Customer Personal Data remains in the possession of Qlik following the Termination Date, Qlik's obligations set forth in this DPA shall survive termination of the Agreement with respect to that portion of the Customer Personal Data until it is eventually deleted.

## 8. MISCELLANEOUS

**8.1 Entire Agreement.** This DPA and the Agreement, where referenced, contain the entire agreement regarding the subject matter thereof and supersede any other data protection/privacy agreements and communications between the Parties concerning the Processing by Qlik of Customer Personal Data in Qlik's performance of the Services.

**8.2 Effect of this DPA.** Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the Parties, including the Agreement and this DPA, the terms of this DPA will control as it relates to Processing of Customer Personal Data. If the Parties have entered into a Business Associate Agreement, that Business Associate Agreement shall govern with respect to U.S. "PHI" as defined thereunder. In the event of a conflict between this DPA and the applicable EEA/UK Third Country lawful transfer mechanism (e.g., 2021 SCCs, DPF)), the relevant Third Country lawful transfer mechanism terms/principles will prevail. This DPA is effective from the Effective Date and only if and for so long as Qlik provides Services under the Agreement. This DPA will terminate, unless otherwise terminated by the Parties, on the Termination Date.

**8.3 Liability.** Subject to Section 2.4.2, the total combined liability of either Party towards the other Party, whether in contract, tort or under any other theory of liability, shall be limited to that set forth in the Agreement as well as any disclaimers contained therein. Any reference in such section to the liability of a Party means the aggregate liability of that Party under the Agreement and this DPA.

**8.4 Third Party Rights.** This DPA shall not confer any rights or remedies to any other person or entity other than the Parties except as to enable the Data Protection Law rights of Data Subjects of Customer Personal Data under this DPA.

**8.5 Updates to this DPA.** Qlik may modify the terms of this DPA, such as to account for future changes in Data Protection Law to enable the continued Processing of Customer Personal Data to carry out the Services and shall do so by way of updating the DPA terms on www.qlik.com. Any future changes to this DPA published by Qlik on its website will become effective once published and shall supersede any previous DPA between the Parties, insofar and only to the extent that those changes (i) are to account for changes under Data Protection Law, which may include to account for revised guidance from a Supervisory Authority, or (ii) to enable an EEA/UK Third Country lawful transfer mechanism, as contemplated under Section 5.5, or (iii) are not less favorable to the Customer (for example, to permit further data types of Customer Personal Data to be uploaded to Qlik Cloud). The Customer is therefore encouraged to keep up to date with these DPA terms at www.qlik.com.

## SCHEDULE 2
## TECHNICAL AND ORGANIZATIONAL MEASURES

Qlik shall undertake appropriate technical and organizational measures for the availability and security of Customer Personal Data and to protect it against unauthorized or unlawful Processing and against accidental or unlawful loss, destruction, alteration or damage, and against unauthorized disclosure or access. These measures, listed below, shall take into account the nature, scope, context and purposes of the Processing, available technology as well as the costs of implementing the specific measures and shall ensure a level of security appropriate to the harm that might result from a Security Incident. Some of the measures below apply to Qlik's general IT infrastructure/practices and may not necessarily apply to Qlik Cloud. While Qlik may alter its measures in line with evolving security practices and risks, and with due regard to the nature of the Processing, Qlik will not materially decrease the overall protections of the Customer Personal Data below the aggregate standard of the measures in this Schedule 2. Customers should stay up to date with Qlik's security measures by visiting its security resources available at www.qlik.com.

1. **Access Controls to Premises and Facilities.** Qlik maintains technical and organizational measures to control access to premises and facilities, particularly to check authorization, utilizing various physical security controls such as ID cards, keys, alarm systems, surveillance systems, entry/exit logging and door locking to restrict physical access to office facilities.

2. **Access Controls to Systems and Data.** Qlik operates technical and organizational measures for user identification and authentication, such as logs, policies, assigning distinct usernames for each employee and utilizing password complexity requirements for access to on-premises and cloud-based platforms. In addition, user access is established on a role basis and requires user management, system or HR approval, depending on use. Second-layer authentication may be employed where relevant by way of multi-factor authentication. User access for sensitive platforms is subject to periodic review and testing. Qlik's IT control environment is based upon industry-accepted concepts, such as multiple layers of preventive and detective controls, working in concert to provide for the overall protection of Qlik's computing environment and data assets. To strengthen access control, a centralized identity and access management solution is used to manage application access. Qlik uses on-boarding and off-boarding processes to regulate access by Qlik Personnel.

3. **Disclosure Controls.** Qlik maintains technical and organizational measures to transport, transmit and communicate or store data on data media (manual or electronic). For certain data transfers, bearing in mind the risk and sensitivity of the data, Qlik may employ encrypted network or similar transfer technologies. Personnel must utilize a dedicated or local VPN network to access internal resources and/or industry-standard authentication and secure communication mechanisms to access cloud-based systems. Logging and reporting are utilized for validation and review purposes. Third party Subprocessors are subject to privacy and security risk assessments and contractual commitments.

4. **Input Controls.** Qlik maintains measures in its general IT systems for checking whether relevant data has been entered, changed or removed (deleted), and by whom, such as by way of application-level data entry and validation capabilities. and reporting is utilized for validation and review purposes. For Qlik Cloud Customer Content, other than as provided for under this DPA, the Customer is solely responsible for entry, alteration and removal (deletion) of any of its Qlik Cloud Customer Content in Qlik Cloud and, to respect the security and integrity of the Customer Personal Data, Qlik does not monitor Qlik Cloud Customer Content for regular entries, alterations or removals (deletion) by the Customer or its users in its use of the Services.

5. **Job Controls.** Qlik uses technical (e.g., access controls) and organizational (e.g., policies) measures to delineate, control and protect data for which the Qlik is the Controller or the Processor. Qlik records and delineates the data types for which it is a Controller or a Processor in its record of processing activities under Article 30 (2) EU GDPR.

6. **Separation Controls.** Qlik uses segregation standards and protocols between production, testing and development environments of sensitive platforms. Additionally, segregation of data is further supported through user access role segregation.

7. **Availability Controls.** Qlik maintains measures to assure data availability such as local and/or cloud-based back-up mechanisms involving scheduled and monitored backup routines, and local disaster recovery procedures. Qlik may supplement these with additional security protections for its business, for example malware protection. Additionally, data centers of a critical nature are required to submit to periodic 3rd party evaluation of operating effectiveness for significant controls ensuring data availability. Relevant systems and data center locations are protected through the use of industry-standard firewall capabilities.

8. **Other Security Controls.** Qlik maintains (i) regular control evaluation and testing by audit (internal and/or external), on an as-needed basis, (ii) individual appointment of system administrators, (iii) user access by enterprise IDP, (iv) binding policies and procedures for Qlik's Personnel, and (v) regular security and privacy training. Policies will clearly inform Personnel of their obligations (including confidentiality and associated statutory obligations) and the associated consequences of any violation.

9. **Certifications**. Qlik has, at the time of the Effective Date, and shall maintain, certifications regarding SOC 2 Type II and ISO 27001 or their equivalents, which may change over time in line with evolving security standards.

10. **Cloud Specific Measures.** Further security measures relating to Qlik Cloud are set out in the Qlik Cloud Information Security Addendum. Security measures in relation to Talend Cloud are set out in the Talend service description guide at https://www.qlik.com/us/legal/product-terms .

## SCHEDULE 3
## SUBPROCESSORS

**For Qlik offerings:**

**Qlik Third Party Subprocessors:**

- Amazon Web Services
- MongoDB
- Salesforce
- Grazitti SearchUnify
- Microsoft
- Persistent
- Altoros
- Ingima
- ISS Consult
- Galil
- Google Firebase
-

**For Talend offerings:**

**Talend Third Party Subprocessors:**

- Amazon Web Services
- Microsoft Azure
- MongoDB
- GitHub
- Intercom
- Atlassian
- Microsoft
- Proofpoint Secure Share
- Salesforce

**Affiliates:**

| Affiliates | Country |
|---|---|
| QlikTech International AB, Talend Sweden AB | Sweden |
| QlikTech Nordic AB | Sweden |
| QlikTech Latam AB | Sweden |
| QlikTech Denmark ApS | Denmark |
| QlikTech Finland OY | Finland |
| QlikTech France SARL, Talend SAS | France |
| QlikTech Iberica SL (Spain), Talend Spain, S.L. | Spain |
| QlikTech Iberica SL (Portugal liaison office), Talend Sucursal Em Portugal | Portugal |
| QlikTech GmbH, Talend Germany GmbH | Germany |
| QlikTech GmbH (Austria branch) | Austria |
| QlikTech GmbH (Swiss branch), Talend GmbH | Switzerland |
| QlikTech Italy S.r.l., Talend Italy S.r.l. | Italy |
| Talend Limited | Ireland |
| QlikTech Netherlands BV, Talend Netherlands B.V. | Netherlands |
| QlikTech Netherlands BV (Belgian branch) | Belgium |
| Blendr NV | Belgium |
| QlikTech UK Limited, Talend Ltd. | United Kingdom |
| Qlik Analytics (ISR) Ltd. | Israel |
| QlikTech International Markets AB (DMCC Branch) | United Arab Emirates |
| QlikTech Inc., Talend, Inc., Talend USA, Inc. | United States |
| QlikTech Corporation (Canada), Talend (Canada) Limited | Canada |
| QlikTech México S. de R.L. de C.V. | Mexico |
| QlikTech Brasil Comercialização de Software Ltda. | Brazil |
| QlikTech Japan K.K., Talend KK | Japan |
| QlikTech Singapore Pte. Ltd., Talend Singapore Pte. Ltd. | Singapore |
| QlikTech Hong Kong Limited | Hong Kong |
| Qlik Technology (Beijing) Limited Liability Company, Talend China Beijing Technology Co. Ltd. | China |
| QlikTech India Private Limited, Talend Data Integration Services Private Limited | India |
| QlikTech Australia Pty Ltd, Talend Australia Pty Ltd. | Australia |
| QlikTech New Zealand Limited | New Zealand |

. Further details are available at, and any changes shall be published to, https://community.qlik.com/t5/Qlik-Technical-Bulletin-Blog/Qlik-Subprocessors-General-Data-Protection-Regulation-GDPR/ba-p/1572352.

## SCHEDULE 4
## 2021 SCCs

*Controller to Processor (Module 2) or Processor to Processor (Module 3)*

### 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 personal 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 I.A (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 I.A (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 I.B.

(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) 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); and

(viii) Clause 18(a) and (b).

(ix) [If the data exporter is a controller:] Clause 8.1(b)

(x) [If the data exporter is a processor:] Clause 8.1(a), (c) and (d) and Clause 8.9 (f) and (g);

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

***Clause 4***

**Interpretation**

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

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

(e) 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 I.B.

### *Clause 7*

### [not used]

## 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.

**MODULE TWO: Transfer controller to processor**

#### 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 I.B, 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 II 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 I.B. 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 II. 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 I.B.

### 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 benefitting 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.

**MODULE THREE: Transfer processor to processor**

**8.1 Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

**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 I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

**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 rectify or erase 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 I.B. 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 controller 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, they 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 subject. 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 or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out in Annex I.B.

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by 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 benefitting 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 of Regulation (EU) 2016/679;

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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

**MODULE TWO: Transfer controller to processor**

(a) 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 at least thirty (30) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

**MODULE THREE: Transfer processor to processor**

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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.

(d) 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.

(e) 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

**MODULE TWO: Transfer controller to processor**

(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.

**MODULE THREE: Transfer processor to processor**

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: 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.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Sweden.

### *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 Sweden.

(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.

## ANNEX I

### A. LIST OF PARTIES

**MODULE TWO: Transfer controller to processor**
**MODULE THREE: Transfer processor to processor**

**Data exporter(s):**

Name: The Customer, as defined in the Agreement.

Address: The address of Customer specified in the Agreement, DPA and/or applicable order form(s) as applicable.

Contact person's name, position, and contact details: The name, position, and contact details of the Customer's contact person specified in the table at the commencement of this DPA.

Activities relevant to the data transferred under these Clauses: transfer of Customer Personal Data, as defined in the DPA, for Processing by the data importer.

Signature and date: [insert signature and date]

Role: controller (module two) or processor (module three).

**Data importer(s):**

Name: Qlik, as defined in the Agreement.

Address: The address of Qlik specified in the Agreement, DPA and/or applicable order form(s) as applicable.

Contact person's name, position, and contact details: Roy Horgan, Senior Director, Privacy Counsel & Data Protection Officer, privacy@qlik.com.

Activities relevant to the data transferred under these Clauses: Processing of Customer Personal Data, as defined in the DPA, on behalf of the data exporter.

Signature and date: [insert signature and date]

Role: processor (module two) or subprocessor (module three).

### B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

See the Details of Processing table at the commencement of this DPA.

*Categories of personal data transferred*

Customer Personal Data as defined in the DPA. See the Details of Processing table at the commencement of the DPA.

*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*

See the Details of Processing table at the commencement of the DPA. Applied restrictions or safeguards are set out in the DPA.

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)*

See the Details of Processing table at the commencement of the DPA.

*Nature of the processing*

See the Details of Processing table at the commencement of the DPA.

*Purpose(s) of the data transfer and further processing*

For the purposes of enabling the data exporter to use the Services in accordance with the Agreement.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

In accordance with any retention periods controlled by the Customer, or if such retention periods are controlled by Qlik, in accordance with the Agreement and the DPA.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

Qlik's Subprocessor details are set out at Schedule 3 to the DPA.

### C. COMPETENT SUPERVISORY AUTHORITY

*Identify the competent supervisory authority/ies in accordance with Clause 13*

The Competent Supervisory Authority of the EU Member State in which the data exporter is established, based on the list available at https://edpb.europa.eu/about-edpb/about-edpb/members_en. In case of ambiguity, this will be the Competent Supervisory Authority of Sweden:

Integritetsskyddsmyndigheten
Drottninggatan 29
5th Floor
Box 8114
104 20 Stockholm

Tel. +46 8 657 6100, Fax +46 8 652 8652, Email: imy@imy.se, Website: http://www.imy.se/

## ANNEX II

### TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

These are as listed in Schedule 2 of the DPA.

## ANNEX III

### LIST OF SUB-PROCESSORS

The Controller has authorised the use of the sub-processors listed in Schedule 3 of the DPA, as updated from time to time.

# Qlik Cloud Acceptable Use Policy

This Qlik Cloud Acceptable Use Policy ("AUP") defines acceptable practices and prohibited uses relating to Qlik's network and systems that are used for hosting Qlik products and services or providing SaaS services (collectively, the "Services") by users ("You" or "Your"). The Services must be used in a manner consistent with the intended purpose of the Services, the terms of Your applicable agreement with Qlik for the products and/or services being hosted and this AUP. Qlik may non-materially modify this AUP by posting a revised version to www.qlik.com. By using the Services, You agree to the latest version of this AUP. For purposes of this AUP, "Qlik" includes QlikTech International AB and its affiliates, and Qlik may be referred to as "We" or "Our."

## 1. Security

- You agree to maintain appropriate security, protection and backup copies of any content that is included, transmitted, stored, published, displayed, distributed, integrated, or linked by You in the Services (collectively, "Content"). We will have no liability of any kind as a result of the deletion of, correction of, destruction of, damage to, loss of or failure to store or backup any Content.
- You may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include:
  - Unauthorized Access. Bypassing, circumventing, or attempting to bypass or circumvent any measures We may use to prevent or restrict access to the Services (or other accounts, computer systems or networks connected to the Services), including any attempt to probe, scan, or test the vulnerability of the Services or to breach any security or authentication measures used by the Services.
  - Reverse Engineering. Deciphering, decompiling, disassembling, reverse engineering or otherwise attempting to derive any source code or underlying ideas or algorithms of any part of the Services, except to the limited extent applicable laws specifically prohibit such restriction.
  - Falsification of Origin or Identity. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route, or attempting to impersonate any of Our employees or representatives.
  - Using manual or automated software, robotic process automation, devices, or other processes to harvest or scrape any content from the Services.
  - Denial of Service (DoS)/Intentional Interference. Flooding a System with communications requests so the System either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective, or interfering with the proper functioning of any System, including by deliberate attempts to overload the System.

## 2. No Illegal, Harmful, or Offensive Use or Content

- You may not use, or encourage, promote, facilitate or instruct others to use, the Services for any illegal (under applicable law), fraudulent, infringing or offensive use, or to transmit, store, display, distribute, post or otherwise make available content that is illegal (under applicable law), harmful, fraudulent, infringing or offensive. Prohibited activities or content include:

    - Illegal, Harmful or Fraudulent Activities. Any activities that are illegal, that violate the rights of others, that may be harmful to others, or that may be harmful to Our operations or reputation.
    - Infringing Content. Content that infringes or misappropriates the intellectual property or proprietary rights of others or that violates any law or contractual duty.
    - Offensive Content. Content that is illegal, harassing, libellous, fraudulent, defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable.
    - Harmful Content. Content or other computer technology that may damage, interfere with, surreptitiously intercept or disrupt the Service, including viruses, Trojan horses, spyware, worms, time bombs, or cancelbots.
    - Unsolicited Content. Content that constitutes unauthorized or unsolicited advertising, junk or bulk e-mail ("spamming") or contains software viruses or any other computer codes, files or programs that are designed or intended to disrupt, damage, limit or interfere with the proper function of any software, hardware, or AUP March 2021 telecommunications equipment or to damage or obtain unauthorized access to any system, data, password, or other information of Ours or any third party.
    - Competitive Content. Attempting to collect and/or publish performance data for the purposes of benchmarking, or developing a product that is competitive with any Our product or services.

**3. Our Monitoring and Enforcement**

- We reserve the right, but do not assume the obligation, to monitor for, and investigate, any violation of this AUP or other misuse of the Services. Failure to comply with this AUP constitutes a material breach of the terms and conditions upon which You are permitted to use the Services, and at any time may result in Qlik taking any and all remedial actions in its sole discretion in accordance with the Contract Disputes Clause, up to and including:
    - Warnings;
    - Suspending or terminating access to the Services;
    - Removing, disabling or prohibiting access to content that violates this AUP and/or Your applicable agreement with Qlik; and/or
    - Legal proceedings against You.

We may report any activity that We suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

We take no responsibility for any material created or accessible on or through the Services and will not exercise any editorial control over such material. We are not obligated to monitor such material, but reserves the right to do so, as well as remove any content that We, in Our sole discretion, determine to be in violation of this AUP.

### 4. Reporting of Violations of this Policy

If You become aware of any violation of this AUP, You will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. Violation of this AUP may be reported to security@qlik.com.

### 5. Subdomains

If You are permitted to choose a Qlik subdomain name for use with Qlik Cloud, such subdomain name may not infringe or violate third-party intellectual property rights or include offensive, obscene, vulgar or other objectionable or unlawful language, and be unique enough to prevent confusion with other entities, brands or trademarks. We reserve the right (but shall have not obligation to) to monitor, reject, revoke or cancel any Qlik subdomain name that is not in compliance with this Policy or any applicable laws.

# QLIK CLOUD GOVERNMENT

## RULES OF BEHAVIOR FOR EXTERNAL USERS

These Rules of Behavior for External Users (“Rules”) defines the responsibilities and expected behavior by users (“You” or “Your”) of QlikTech Inc.’s (“Qlik”) network and systems that are used for hosting Qlik Cloud Government SaaS Services ("QCG") QCG must be used in a manner consistent with the intended purpose of QCG, the terms of Your applicable agreement with Qlik for QCG and these Rules. By using QCG, you agree to the latest version of these Rules.

1. You must report all security incidents or suspected incidents to the Qlik Customer Support Team (government.support@qlikcloudgov.com). Reports of any anomaly / possible security incidents are immediately analyzed and mitigated by the Information Security team.
2. As a Qlik customer, You are in sole control of the individual permissions on Your accounts and surveys, which enables integrity of the systems that You access.
3. You must meet Your agency’s password policy.
4. You must not store passwords or other sensitive information on desks or in plain sight. Passwords may not be shared, and must be protected at all times.
5. You must never share account information details with anyone from Qlik except members of the Qlik Customer Support Team government.support@qlikcloudgov.com)if you require their assistance. You should only share the information after ensuring that the parties have the proper clearance, authorization, and need-to-know.
6. You must never leave your computer unattended while logged into QCG.
7. You own all right, title and interest in all data you enter into QCG, including uploaded content such as completed forms and documents. All reports and downloads that are derived from the data are also owned by you. All data specified is deemed as Confidential information and will not be utilized by Qlik for any purpose.
8. You are solely responsible for all data, and are liable for Your data and the manner in which You collect or distribute your data to third parties.
9. You must not resell QCG or permit third parties to use QCG without prior written consent.
10. You must not make unauthorized copies of any content within QCG except your own data.
11. You must not upload data that contains nudity, pornography, profanity, or foul language or links to such content.
12. You must not upload or store malicious software or data that condones, promotes, contains or links to warez, cracks, hacks, their associated utilities, or other piracy related information, whether for educational purposes or not.

13. You must not upload data that infringes any copyrights, patents, trademarks or other Intellectual property.

14. You must not upload binary files or executable files.

15. You must use browsers using TLS 1.2, which use AES 128/256-bit encryption.

16. You must not reverse-engineer or tamper with the security of QCG.

17. You must not perform vulnerability tests, network scans, penetration tests or other investigative techniques on QCG services.

18. You must report a suspected security breach event to government.support@qlikcloudgov.com. In such a case, Qlik will provide reasonable assistance to mitigate further exposure and attempt to determine the root cause.

19. You agree to contact the Qlik Customer Support Team (government.support@qlikcloudgov.com) if you do not understand any of these Rules.

20. You acknowledge and accept that any violation of these Rules may subject You to civil and/or criminal actions and that Qlik retains the right, , to terminate, cancel or suspend Your access rights to QCGin accordance with the Contract Disputes Act, in the event of Your violation of these Rules.