QLIK® DATA PROCESSING ADDENDUM

This DPA version is for information purposes only and is not valid for execution. Any executed copies received shall not be binding. Customers wishing to execute a Qlik DPA must do so using the DocuSign version found at https://www.qlik.com/us/legal/legal-agreements

This Data Processing Addendum including its Schedules 1, 2 and 3 ("**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. If the Customer makes any deletions or other revisions to this DPA, those deletions or revisions are hereby rejected and invalid. The Customer's signatory represents and warrants that he or she has the legal authority to bind the Customer to this DPA.

INSTRUCTIONS

This DPA has been presigned by Qlik. In order for this DPA to be effective, the Customer must complete and sign the information block below with the Customer full legal entity details and signatory information. The Customer will then receive a fully executed version to the email address it enters in the completion process.

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	xxxxxxxxxxxxxxxxxxx	*Customer legal name (include entity type, e.g., Inc., Ltd., etc.)*	xxxxxxxxxxxxxxxxxxx
		Country of customer	xxxxxxxxxxxxxxxxxxx
Position	xxxxxxxxxxxxxxxxxxx	*Name of signatory*	xxxxxxxxxxxxxxxxxxx
Signature	xxxxxxxxxxxxxxxxxxx	*Position*	xxxxxxxxxxxxxxxxxxx
Date	xxxxxxxxxxxxxxxxxxx	*Signature*	xxxxxxxxxxxxxxxxxxx
		Date	xxxxxxxxxxxxxxxxxxx
Key privacy contact	xxxxxxxxxxxxxxxxxxx	*Key privacy contact*	xxxxxxxxxxxxxxxxxxx

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 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 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, Qlik 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 Japan Act on the Protection of Personal Information, the Singapore Personal Data Protection Act, the UK Data Protection Act 2018 and UK General Data Protection Regulation, and the 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. It does not include any Industry-Specific Data Law.

"**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.

"**Industry-Specific Data Law**" means any Data Protection Law that is specific to Customer's industry, including the Health Insurance Portability and Accountability Act and its implementing regulations ("HIPAA") and the Gramm Leach Bliley Act ("GLBA"), and any industry data standard to which Customer has agreed to comply, including the Payment Card Industry Data Security Standard of the PCI Security Standards Council ("PCI DSS").

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

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

"**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.

"**Services**" 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 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 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 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 of Customer files via Qlik's support portal on the Qlik Community website.

"**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 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 5.3 of this DPA."**UK Customer Personal Data**" means Customer Personal Data that is subject to the UK GDPR.

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

"**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. 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**" 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	Data analysis and storage of Customer Personal Data by the Customer in Qlik Cloud and/or 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 as long as such data is not regulated by an Industry-Specific Data Law.
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 the 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 the Customer Personal Data only to perform the Services for the Customer and for no other purpose. To the extent that the CCPA applies to the Processing of Customer Personal Data in the course of providing the Services, Qlik is a Service Provider and the Customer is a Business. 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.

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 5.5 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). If a governmental body sends Qlik such a demand for Customer Personal Data, Qlik will attempt, where possible under relevant law, to redirect the governmental body to request that data directly from the Customer. Qlik does not sell Customer Personal Data. The Customer will not disclose Personal Data to Qlik or request that Qlik Process Customer Personal Data that is subject to any Industry-Specific Data Law without first notifying Qlik and agreeing upon any additional written terms applicable to the Processing of such Industry-Specific Data Law. For clarity, Qlik expressly disclaims any responsibility under this DPA for the Processing of Personal Data under any Industry-Specific Data Law. Qlik has no obligation to assess the Customer Personal Data in order to identify information subject to any Industry-Specific Data Law.

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 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 accidental or unlawful loss, destruction, alteration or damage, and against unauthorized disclosure or access. 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 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 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;

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 are hereby incorporated in this DPA, as applicable, and shall apply as described in Section 5.2 below and subject to the provisions of this DPA.

5.2 Particulars regarding the 2021 SCCs. The 2021 SCCs referred to in Section 5.1 above shall apply with the following particulars:

5.2.1 the Customer will be the data exporter and Qlik will be the data importer;

5.2.2 for Clause 9 (a) (use of Subprocessors), the Parties agree to option 2 (general written authorization) as described in Section 4. A list of Qlik's Subprocessors , for the

purpose of Annex III to the 2021 SCCs, is available at Schedule 3;

5.2.3 the options in Clause 7 (docking) and Clause 11 (a) (redress) are not exercised;

5.2.4 for Clause 17 (governing law), Clause 18 (b) (choice of forum and jurisdiction) and Annex I (c) (Supervisory Authority), the Parties agree that the governing law, relevant Supervisory Authority, and relevant courts for a dispute regarding the 2021 SCCs will be those of the Customer country (or state, if relevant) if the Customer is an EEA entity and, in any event, decided in accordance with the relevant Data Protection Law. In the event of ambiguity, the governing law, Supervisory Authority and relevant courts will be those of Sweden;

5.2.5 the Parties agree that the aggregate liability of Qlik to the Customer under or in connection with this DPA and the 2021 SCCs will be limited as set out in Sections 2.4.2 and 8.3;

5.2.6 the Parties agree that any rights to audit pursuant to Clause 8.9 of the 2021 SCCs will be exercised in accordance with Section 6;

5.2.7 the Processing details to be provided in Annex I of the 2021 SCCs are provided in Section 2; and

5.2.8 the Technical and Organizational Measures to be provided in Annex II of the 2021 SCCs are provided in Schedule 2.

5.3 Transfers of 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, the Parties agree that the provisions of the UK Addendum shall apply to such transfers. In particular:

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

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

5.3.3 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;

5.3.4 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 of this DPA and the selection and disapplication of optional clauses as set out in Sections 5.2.2 and 5.2.3 of this DPA);

5.3.5 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

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

5.4 Alternative Lawful Transfer Mechanisms. The Customer acknowledges that Qlik's obligations under the 2021 SCCs and/or the UK Addendum 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 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.

5.5 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 5.5 does not overwrite Clause 15 (where applicable) of the 2021 SCCs or the equivalent protection under the UK Addendum.

5.6 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 Requests. Without prejudice to its other obligations in this DPA, Qlik will give to the Customer on written request (where such requests shall occur no more than once every 12 months) reasonable information necessary to determine Qlik's compliance with this DPA and will discuss in good faith any audits reasonably required by the Customer, conducted by a third party agreed to by the Parties. Such audits, if agreed, must be carried out at the Customer's cost, be conducted in a manner undisruptive to the business of Qlik and its Affiliates, be conducted subject to the terms of an applicable non-disclosure agreement, and not prejudice other confidential information (including but not limited to Personal Data) of Qlik, its Affiliates or its other customers.

6.2 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 of Qlik Cloud due to an issue within Qlik's control (for example, exceeding 10 working days), 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. In the event of a conflict between this DPA and the applicable 2021 SCCs (Modules Two or Three) and/or the UK Addendum, the relevant 2021 SCCs and/or the UK Addendum 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 5.2, 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 Breach. 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. Qlik Cloud Specific Measures. Further security measures relating to Qlik Cloud are set out in the Qlik Cloud Information Security Addendum at https://www.qlik.com/us/legal/product-terms.

SCHEDULE 3
SUBPROCESSORS

Qlik Affiliates:

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

Third Party Subprocessors:

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

Further Subprocessor details are available at https://community.qlik.com/t5/Qlik-Technical-Bulletin-Blog/Qlik-Subprocessors-General-Data-Protection-Regulation-GDPR/ba-p/1572352 .