Last Updated: July 4, 2025

This Data Processing Addendum represents an addendum to Company's (also referred as "**You**") existing commercial agreement with GoodData governing Company's use of GoodData products or services ("**Agreement**") (each, a "**Party**" and together, the "**Parties**") ("**Addendum**") and is hereby incorporated into the Agreement. In the event of any conflict between this Addendum and any data processing terms contained in the Agreement between the Parties, the terms of this Addendum regarding the processing of Personal Data shall control and supersede the terms set forth in the Agreement.

1. Definitions.

All capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement or the Applicable Data Protection Law, as applicable.

1.1. **Applicable Data Protection Law** means all applicable international, federal, national and state privacy and data protection laws that apply to the processing of Personal Data that is the subject matter of the Agreement (including, where applicable, the EU Protection Law, the Act on Federal Data Protection of 1 September 2023 and its Ordinance ("**Swiss DPA**"); the Data Protection Act 2018 (c. 12) of the United Kingdom; and the CCPA).

1.2. **CCPA** means the California Consumer Privacy Act of 2018 (as amended by California Privacy Rights Act of 2020), Cal. Civil Code § 1798.100 et seq.

1.3. **Controller** means the entity that determines the purposes and means of the processing of Personal Data.

1.4. **EEA** means European Economic Area.

1.5. **EU** means European Union.

1.6. **EU Data Protection Law** means inter alia the EU General Data Protection Regulation 2016/679 ("GDPR") and any applicable national laws made under the GDPR.

1.7. **Highly Sensitive Personal Data** means user passwords/secrets, social security numbers, driver license numbers, bank account numbers or any data subject to Payment Card Industry Data Security Standard (PCI-DSS).

1.8. **Personal Data** means Customer Data and/or Support Data that is "personal data," "personal information," "personally identifiable information," or an equivalent term, as defined by Applicable Data Protection Law.

1.9. **Processor** means an entity that processes Personal Data on behalf of the Controller.

1.10. **Security Breach** means an unlawful or unauthorized use or acquisition of Personal Data due to GoodData's failure to comply with the GoodData Security Program with respect to the Subscription or Support Services. The term Security Breach always excludes: (a) unsuccessful attempts to penetrate computer networks or servers maintained by or for GoodData; and (b) immaterial incidents that occur on a routine basis, such as security scans, brute-force attempts or "denial of service" attacks, and (c) GoodData's good-faith receipt of Highly Sensitive Personal Data or Sensitive Personal Data in violation of restrictions on Personal Data processing as further specified by the Agreement.

1.11. **Sensitive Personal Data** means (i) Protected Health Information subject to the Health Insurance Portability and Accountability Act ("**HIPAA**") (where "**Protected Health Information**" or "**PHI**" has the meaning set forth in HIPAA); and/or (ii) Special Categories of Personal Data (as defined by Applicable Data Protection Law, including the GDPR or similar concepts under the California Consumer Privacy Act) or such other personally identifiable information or data.

1.12. **EU Standard Contractual Clauses** means the annex found in Commission Implementing Decision (EU) 2021/914 of 4 June

2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (available as of the Addendum effective date at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj or any subsequent link published by the competent EU authorities). In the event of any conflict between the EU Standard Contractual Clauses and this Addendum, the EU Standard Contractual Clauses shall control and supersede.

2. Data Protection.

2.1. **Relationship of the Parties.** As between the Parties and for the purposes of this Addendum, (i) Company is the Controller and appoints GoodData as a Processor to process the Personal Data; and/or (ii) Company is the Processor of Personal Data and Company appoints GoodData as its Subprocessor to provide it with subprocessing activities; as described in Annex I.

2.2. **Purpose Limitation.** GoodData shall process the Personal Data only for the purposes described in Annex I hereto and in accordance with Company's documented instructions (the "**Permitted Purpose**"). Company agrees and acknowledges that it will not process any Highly Sensitive Personal Data under the Agreement. Notwithstanding the foregoing and where applicable, GoodData may offer Company an additional security and compliance add-on(s) intended for the processing of Sensitive Personal Data as defined herein. Further, GoodData will immediately inform Company if, in its opinion, any Company instruction infringes Applicable Data Protection Laws.

2.3. **International transfers of Personal Data**. Company acknowledges that GoodData and its Subprocessors may process Personal Data in countries that are outside the EEA, United Kingdom, and Switzerland (EEA, United Kingdom, and Switzerland hereafter together as "**European Countries**"). GoodData will at all times provide an adequate level of protection for the Personal Data, wherever processed, in accordance with the requirements of Applicable Data Protection Law. If Personal Data is transferred from European Countries to outside the EEA, the following shall apply:

- If the registered office of GoodData is located outside the EEA, Company shall be the data exporter and GoodData shall be the data importer.

- If the registered office of GoodData is located within the EEA, GoodData will be the data exporter for onward transfers to outside the EEA.

2.4. **EU Standard Contractual Clauses and Switzerland**. Where (i) Company is the data exporter (see section 2.3.), (ii) GDPR or Swiss DPA apply to international data transfers from EEA / Switzerland to countries outside the EEA and (iii) an international transfer of Personal Data cannot take place on the basis of an adequacy decision pursuant to Art 45 (3) GDPR and (iv) GoodData is not subject to the GDPR for the relevant processing activities as described in Annex I, Parties will comply with the obligations in the EU Standard Contractual Clauses, which shall form an integral part of this Addendum. For the purposes of EU Standard Contractual Clauses:

2.4.1. in Clause 7, the optional docking clause will not apply;

2.4.2. in Clause 11, the optional language on lodging a complaint with an independent dispute resolution body will not apply;

2.4.3. the Parties choose Option 1 in Clause 17 (Governing Law) and complete the Clause 17 with the following: *"These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Czech Republic."*;

2.4.4. the Parties agree to complete the Clause 18(b) (Choice of Forum and Jurisdiction) with the following: “The Parties agree that those shall be the courts of Czech Republic.”; and

2.4.5. Annexes I and II of this Addendum are hereby deemed as Annexes I and II of the EU Standard Contractual Clauses.

Where (i) GoodData is the data exporter (see section 2.3.), (ii) GDPR or Swiss DPA apply to international data transfers from EEA / Switzerland to countries outside the EEA and (iii) an international transfer of Personal Data cannot take place on the basis of an adequacy decision pursuant to Art 45 (3) GDPR, GoodData will enter into respective EU Standard Contractual Clauses as the case may be with data importers outside the EEA.

To the extent Personal Data solely subject to the Swiss DPA is to be internationally transferred, all references to the GDPR within the EU Standard Contractual Clauses shall be understood to be references to the Swiss DPA and the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority.

United Kingdom. To the extent international transfer of Personal Data is subject to Applicable Data Protection Law in the United Kingdom (including UK GDPR and Data Protection Act 2018) (“**UK Data Protection Laws**”), for so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of Personal Data to processors set out in the European Commission’s Decision 2010/87/EU (“**Prior SCCs**”), the Prior SCCs shall apply between Company and GoodData on the following basis: (i) Appendix I and II of the Prior SCCs shall be deemed completed with the relevant information set out in Annex I and II to this Addendum; (ii) references in the Prior SCCs to “the law of the Member State in which the data exporter is established” shall be deemed to mean “the laws of England and Wales”; (iii) the optional illustrative indemnification clause will not apply; and (iv) any other obligation in the Prior SCCs determined by the Member State in which the data exporter is established shall be deemed to refer to an obligation under UK Data Protection Laws. Where the Prior SCCs do not apply and the Parties are lawfully permitted to rely on the EU Standard Contractual Clauses for transfers of Personal Data from the United Kingdom subject to completion of a UK Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner’s Office under s.119A(1) of the Data Protection Act 2018 which can be found at https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf (“**UK Addendum**”), then the EU Standard Contractual Clauses, completed as set out in this Addendum shall also apply to transfers of such Personal Data, subject to the provision that the UK Addendum shall be deemed executed between GoodData and Company, and the EU Standard Contractual Clauses shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data. If neither the Prior SCCs or UK Addendum with EU Standard Contractual Clauses applies, then the Parties shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the UK Data Protection Laws without undue delay.

2.5. **Confidentiality of Processing.** GoodData shall ensure that any person that it authorises to process the Personal Data (including GoodData's affiliates and their staff, agents and subcontractors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Personal Data who is not under such a duty of confidentiality. GoodData shall ensure that only Authorised Persons will process the Personal Data, and that such processing shall be limited to the extent necessary to achieve the Permitted Purpose. GoodData accepts responsibility for any breach of this Addendum caused by the act, error or omission of an Authorised Person.

2.6. **Prohibition on Selling and/or Sharing Information of California residents.** For avoidance of doubt, GoodData is a Service Provider and not a Third Party as defined by the CCPA. Therefore, GoodData shall not: (i) sell or share the Personal Data; (ii) retain, use, or disclose the Personal Data for any purpose other than providing the services specified in the Agreement or for a Business Purpose. Specifically, GoodData shall not retain, use, or disclose the Personal Data for a Commercial Purpose; or (iii) retain, use, or disclose the Personal Data outside of the direct business relationship between GoodData and Company. Notwithstanding anything in the Addendum or any related order form or other document, the Parties acknowledge and agree that Company's provision of access to Personal Data is not part of and explicitly excluded from the exchange of consideration, or any other thing of value, between the Parties.

2.7. **Security**. GoodData shall implement appropriate technical and organisational measures to protect the Personal Data from a Security Breach. At a minimum, such measures shall include the security measures identified in Annex II to this Addendum, and as further described in the Documentation. Where there is an unlawful or unauthorized use or acquisition of Personal Data in systems entirely controlled by GoodData, or GoodData discovers any unauthorized use or acquisition of Personal Data in any third party systems that are processing Personal Data on GoodData's behalf, GoodData will promptly notify Company of such breach and promptly investigate.

2.8. **Subprocessing.** Company authorizes GoodData to engage its Affiliates and third parties to process its Personal Data ("**Subprocessors**") listed at https://www.gooddata.com/subprocessors ("**GoodData List of Subprocessor(s)**"), provided that GoodData provides at least thirty (30) days' prior written notice of the addition of any Subprocessor (including the categories of Personal Data processed, details of the processing it performs or will perform, and the location of such processing) by means of a notice on the aforementioned GoodData List of Subprocessors site. We encourage Company to periodically review the GoodData List of Subprocessors site for the latest information on GoodData Subprocessor practices, and especially before Company provides GoodData with any Personal Data. Company may sign up to receive email notification of any such changes to the GoodData List of Subprocessors on the https://www.gooddata.com/subprocessors site. Company has the opportunity to object to such changes within 30 days after written notification. If Company objects to GoodData's appointment of a new Subprocessor on reasonable grounds relating to the protection of its Personal Data, then the Parties will promptly confer and discuss alternative arrangements to enable GoodData to continue processing of Personal Data. In all cases, GoodData shall impose in writing the same data protection obligations on any Subprocessor it appoints as those provided for by this Addendum and GoodData shall remain liable for any breach of this Addendum that is caused by an act, error or omission of its Subprocessor to the extent it is liable for its own acts and omissions under the Agreement. *For the purposes of the EU Standard Contractual Clauses, the Parties agreed to Option 2 (General Prior Authorization) in the Clause 9 (Use of subprocessors) for both, MODULE TWO: Transfer controller to processor and MODULE THREE: Transfer processor to processor.*

2.9. **Cooperation and Individuals' Rights.** If Company is unable to directly respond to a privacy inquiry made by a Data Subject itself, GoodData shall, taking into account the nature of the processing, provide all reasonable and timely assistance to Company by appropriate technical and organisational measures, insofar as this is possible, to enable it to respond to: (i) any request from Data Subject to exercise any of its rights under Applicable Data Protection Law; and (ii) any other correspondence, enquiry or complaint received from an individual, regulator, court or other third party in connection with the processing of the Personal Data. If any such communication is made directly to GoodData, GoodData shall promptly inform Company providing full details of the same and shall not respond to the communication unless specifically required by law or authorized by Company.

2.10. **Data Protection Impact Assessment.** If GoodData believes or becomes aware that its processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall promptly inform Company of the same. GoodData shall, taking into account the nature of processing and the information available to GoodData, provide Company with all such reasonable and timely assistance as Company may require in order to conduct a data protection impact assessment, and, if necessary, to consult with its relevant data protection authority.

2.11. **Security Breach.** Upon becoming aware of a Security Breach, GoodData shall inform Company without undue delay and shall, taking into account the nature of processing and the information available to GoodData, provide all such timely information and cooperation as Company may reasonably require in order for Company to fulfill its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law and relevant contractual obligations owed by Company to its Users. GoodData shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Breach and shall keep Company informed of all developments in connection with the Security Breach. GoodData shall not notify any third parties of a Security Breach unless and to the extent that: (a) Company has agreed to such notification, and/or (b) notification is required to be made by GoodData under Applicable Data Protection Laws.

2.12. **Deletion or Return of Personal Data.**

2.12.1. In scenarios 2.1.(i) and (ii) *(and, if applicable in Module 2 and 3 of the EU Standard Contractual Clauses)*, the period for which the Personal Data will be retained is the duration of the Agreement.

- Upon termination or expiry of the Agreement, GoodData shall (at Company's election) destroy or enable Company to retrieve all Personal Data in its possession or control as Processor (including any Personal Data subcontracted to a third party for processing).

- Providing Company services includes provision of data storage/warehouse and unless agreed otherwise by the Parties, GoodData shall enable Company to retrieve its Personal Data within thirty (30) days of Company's Agreement termination or expiry.

- GoodData shall delete all Personal Data within ninety (90) days of the termination of this Addendum or the Agreement, or upon Company's written request.

2.12.2. These requirements shall not apply to the extent that GoodData is required by applicable law to retain some or all of the Personal Data, in which event GoodData shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

2.13. **Compliance Assessments.** No more than once per year, solely for the purpose of meeting its audit requirements under the Applicable Data Protection Laws, Company may request an audit in writing. GoodData shall then permit Company (or its appointed third-party auditors) to review the applicable audit records and other relevant security and compliance documentation. Company will be entitled to this information once in any twelve (12) calendar month period, except if and when required by the instruction of a competent data protection authority. Company agrees that the report and other documentation will be used as the primary and only mechanism to audit and inspect GoodData's processing activities, unless Company is required to perform an on-site audit by the applicable data protection authority, or if GoodData materially fails to comply with Applicable Data Protection Laws negatively impacting Company's Personal Data. In the event that Company requires an on-site audit of the procedures relevant to the protection of its Personal Data, then such audits requested must meet the following requirements:

2.13.1. Any audit must be requested with at least thirty (30) days prior notice and include a detailed audit plan that describes the proposed scope, duration, reimbursement rates, and start date of the audit which the Parties must mutually agree upon prior to the commencement of an audit. Audit requests must be sent to security@gooddata.com.

2.13.2. The auditor must execute a written GoodData form nondisclosure agreement prior to conducting the audit.

2.13.3. The audit must be conducted during GoodData's regular business hours, subject to GoodData's policies, and may not unreasonably interfere with GoodData's business activities.

2.13.4. Company will reimburse GoodData for any time expended at its then-current reasonable Ancillary/Professional Services rates, made available to Company upon request. All reimbursement rates will be reasonable and take into account the resources expended by GoodData.

2.13.5. For all audits, Company must immediately notify GoodData with information regarding any suspected or actual non-compliance revealed during an audit. Any information resulting or derived from any audit under this Section including any Company's analyses, notes, assessments or other materials in whatever form or media constitute GoodData Confidential Information subject to applicable protections defined in the Agreement.

2.14. **General Cooperation to Remediate.** In the event that Applicable Data Protection Law, or a data protection authority or regulator, provides that the transfer or processing of Personal Data under this Addendum is no longer lawful or otherwise permitted, then the Parties shall agree to remediate the processing (by amendment to this Addendum or otherwise) in order to meet the necessary standards or requirements. If GoodData is unable to remediate the processing within the applicable cure period set forth in the Agreement, then Company will be entitled to terminate the Agreement (and any other agreement between the Parties relating to the provision of services by GoodData to Company) in accordance with the respective termination provisions of the Agreement.

3. Company Affiliates.

GoodData obligations set forth herein will extend to Company Affiliates to which Company provides access to the Services or Software or whose Personal Data is processed within the Services or Support Services, subject to the following conditions:

3.1. **Compliance**. Company shall at all times be liable for Company Affiliates' compliance with this Addendum and all acts and omissions by Company Affiliate are considered Company's acts and omissions.

3.2. **Claims**. Company Affiliates will not bring a claim directly against GoodData. In the event Company Affiliate wishes to assert a valid legal action, suit, claim or proceeding against GoodData (an "**Affiliate Claim**"): (i) Company must bring such Affiliate Claim directly against GoodData on behalf of such Company Affiliate, unless the Applicable Data Protection Laws require that Company Affiliate be a party to such Affiliate Claim; and (ii) all Affiliate Claims will be considered claims made by Company and are at all times subject to any aggregate limitation of liability set forth in the Agreement.

3.3. **Affiliate Ordering**. If Company Affiliate licenses a separate instance of the respective GoodData Services under the terms of the Agreement, then such Company Affiliate will be deemed a party to this Addendum and shall be treated as Company under the terms of this Addendum.

3.4. **Communication**. Unless otherwise provided in this Addendum, all requests, notices, cooperation, and communication, including instructions issued or required under this Addendum (collectively, "**Communication**"), must be in writing and between Company and GoodData only and Company shall inform the applicable Company Affiliate of any Communication from GoodData pursuant to this Addendum. Company shall be solely responsible for ensuring that any Communication Company provides to GoodData relating to Personal Data for a Company Affiliate reflects the relevant Company Affiliate's intentions. Company warrants and represents that Company is and will at all relevant times remain duly and effectively authorized to give instructions on behalf of each relevant Company Affiliate.

4. Liability.

4.1. **Liability Cap**. Subject to Section 4.2. (Liability Cap Exclusions), the total combined liability of either Party and its Affiliates towards the other Party and its Affiliates under or in connection with the Agreement and this Addendum combined will be limited to the agreed Liability Cap for the relevant Party under the Agreement.

4.2. **Liability Cap Exclusions**. Nothing in Section 4.1. (Liability Cap) will affect the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability).

5. Term.

5.1. The obligations placed upon the GoodData under this Addendum shall survive so long as GoodData and/or its Subprocessors process Personal Data as described herein and/or under the terms of the Agreement.

5.2. Unless there is a separately negotiated data processing agreement between the Parties, in which case the terms of such agreement shall control, this Addendum sets forth the entire agreement and understanding of the Parties relating to the subject matter contained herein and merges all prior discussions and agreements between them, and no Party shall be bound by any representation other than as expressly stated in this Addendum or a written amendment to this Addendum signed by authorized representatives of

each of the Parties.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Company as defined under the Agreement

Address: Address provided by Company during the registration process or in the Agreement

Contact person's name, position and contact details: as provided during Company's registration or in the Agreement

Activities relevant to the data transferred: performance of the Agreement

Role (controller/processor): Controller and/or Processor

Data importer(s):

Name: GoodData Corporation

Address: 135 Main Street, Suite 550, San Francisco, CA 94105

Contact person's name, position and contact details: Vojtech Luhan, Head of Security & Compliance, privacy@gooddata.com

Activities relevant to the data transferred: performance of the Agreement

Role (controller/processor): (Sub)Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may transfer Personal Data to data importer, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons);
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors; and
- Employees, agents, advisors, freelancers of data exporter (who are natural persons).

Categories of personal data transferred

Data exporter may transfer Personal Data to data importer, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title

- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data (including but not limited to home addresses, personal phone numbers, resumes, attendance records, bank details)
- Connection data
- Localisation data
- Support Data

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.

Transfer of sensitive data, if applicable and agreed upon in the Agreement, is done subject to additional safeguards that fully take into account the nature of such data and risks involved. Refer to Annex II.

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

The Personal Data is being transferred on a continuous basis; the frequency is at data exporter's discretion.

Nature of the processing

The nature of processing is storage, modification, distribution and retrieval of Personal Data relating to the provision of services by the data importer to data exporter.

Purpose(s) of the data transfer and further processing

The objectives of processing of Personal Data by the data importer is provisioning of Services by the data importer to the data exporter pursuant to the Agreement (including but not limited to maintaining information security of the Services and ensuring compliance of end users with the terms and conditions, processing of aggregated and pseudonymized Personal Data necessary for analysis of usage of various service capabilities for the purpose of operations and improvement of the Services.

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

As described in the Section 2.12 of the Addendum.

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

The Personal Data are transferred to further Subprocessors for the following purposes:

- Provision of infrastructure and/or software as a service
- Provision of the professional services pursuant to Agreement between data exporter and data importer

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the supervisory authority that is competent to act as lead for Company (as data exporter).

ANNEX II

PRODUCT: GOODDATA PLATFORM - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. **Definitions**. All capitalized terms used in this Annex II shall have the meanings given to them below. All terms not defined herein are as defined in the Agreement.

1.1. **Workspace**: means an analytic container instance within the GoodData Subscription Services.

2. **GoodData Security Standards**. GoodData applies industry-standard security practices to GoodData Technology, via hosted web services (hereinafter referred to as "**Subscription Services**" or the "**Platform**"), as described in greater detail below. This Annex summarizes GoodData's security practices as of the date indicated above.

3. **Compliance**. GoodData's Platform security builds upon the following information security related certifications, industry standards and legislation. Relevant documents demonstrating GoodData's compliance are available to GoodData current and potential customers subject to appropriate confidentiality obligations.

3.1. **Information Security Standards**

3.1.1. **SOC 2 Type II**. GoodData undertakes SOC 2 Type II audits on a regular basis. The SOC 2 reflects current industry standard security best practices. Accordingly, if there is any conflict between the SOC 2 and this Annex II, the SOC 2 terms shall prevail.

3.1.2. **ISO 27001:2013**. GoodData has established its own internal information security management system in line with the requirements and recommendations of ISO 27001:2013 and ISO 27002:2013.

3.1.3. **OWASP**. Open Web Application Security Project ("**OWASP**") provides a set of tools and documentation for building secure web applications. GoodData secure coding guidelines and procedures as well as GoodData web application penetration and vulnerability testing are based on OWASP standards. (See Section 12 below for additional information about web penetration testing using the OWASP guidelines.)

3.2. **Privacy Compliance**: GoodData has implemented and maintains appropriate measures to ensure information security appropriate to the risks related to Personal Data processed in the Platform, to the extent that such Personal Data has been submitted to the Subscription Services in accordance with the Agreement.

4. **Risk Management**

4.1. GoodData has established a Risk Management policy and applies a formal security risk management process to all GoodData information assets.

4.2. GoodData conducts industry standard annual risk assessment. The scope includes systems, applications, networks and data storage and any GoodData process or procedure by which these facilities are administered or maintained, regardless of whether provided, managed or operated by GoodData or by a third party.

5. Hosting Security. Depending on the datacenter, the Platform may be hosted in a private cloud or public cloud.

5.1. **Private Cloud data centers** are third party data center providers' hosting facilities. GoodData has directly entered into "Managed Colocation Service" agreement that provides GoodData, its customers and partners a private cloud built to GoodData's specifications and requirements inside hosting party's facilities. The Managed Colocation Service includes highly secure, scalable and redundant data centers and network, 24x7x365 monitoring and support, and industry-leading service levels; all certified with industry standard security certifications including ISO 27001 and SOC 2 Type II. Under this arrangement, GoodData retains operational control of its hosted infrastructure, procuring only physical hardware from the provider. The provider at no times has access to log on to any GoodData system.

5.2. **Public Cloud data centers** are hosted in highly secure and available facilities of IaaS providers. Under this arrangement, the provider manages the underlying hardware infrastructure, including but not limited to its physical security, and GoodData Operations manage the virtual layers. Segmentation from other customers of the IaaS provider is ensured by following best practices for virtual private clouds including virtual networks, security groups and firewall, and encryption controls. The IaaS providers maintain industry standard security certifications including ISO 27001 and SOC 2 Type II.

6. **Multi-Layered Security**. GoodData addresses data security across all system layers: physical, application, metadata, data, and user access. All external communications are managed over Transport Layer Security ("**TLS**"). Hypertext Transfer Protocol Secure ("**HTTPS**") communications and include industry standard session protection mechanism. Internal communications are managed over TLS, except for internal cluster communications, which are protected by firewalls, split into separate dedicated security zones and require non-encrypted communications for performance reasons.

6.1. **Extensible Security Model.**

6.1.1. **Failover/Redundancy**. Basic data redundancy is built into the hosting services in use. Virtualized storage prevents a single point of failure, while replication and provisioning are managed automatically.

6.1.2. **Data Store Security/Data at Rest**. Data is stored in the GoodData secure storage warehouse and employs industry standard technical and organizational safeguards to protect the secure storage warehouse, including full encryption at rest on the file system level. The meta-model and data are logically separated, and each Workspace is a separate physical object.

6.1.3. **Encryption in Motion; General Encryption Standards**. All data transfers outside of the Platform (including, but not limited to, transfers to the web application and to external backup storage) are subject to specified encryption capabilities, including web-based communications with the Platform, are encrypted using 128-bit or stronger TLS encryption. In environments that require encryption, strong security keys are used with industry-standard encryption algorithms (including

RSA, AES).

6.2. **Operating System Security**. GoodData utilizes hardened versions of Linux® with a minimum set of installed packages, automated deployment mechanisms, ongoing monitoring and alerting and regular, real-time monitoring and system health checks capabilities. GoodData regularly reviews and applies security updates developed internally or by trusted third parties. Formal internal service level commitments are defined for vulnerability management and monitored by GoodData personnel.

6.3. **Security Zones**. The security model involves partitioning the Platform into security zones within the data center.

6.3.1. Only the web tier can receive and respond to requests from outside of the Platform. All web-based interactions with the web tier are authenticated over HTTPS, and additional security precautions are in place to protect communications over this channel.

6.3.2. All other security zones within the Platform are prevented from receiving requests outside of the Platform.

6.3.3. For security purposes, only one layer contained in a separate security zone interacts with the web tier. The components in this zone manage communications between the web tier and the rest of the Platform.

6.3.4. Behind the communications layer, the GoodData middleware and backend components are isolated in their own security groups.

6.3.5. Firewalls are configured to deny all traffic by default, except explicitly designated traffic.

6.4. **Intrusion Prevention, Intrusion Detection and Data Loss Prevention**. GoodData maintains a comprehensive Data Loss Prevention program, which includes a combination of tools and platforms, technical safeguards, access control rules and ongoing monitoring, oversight and log review by an independent security department. GoodData employs an IDS/IPS system directly on the Platform network entry point.

6.5. **Database Security**. GoodData database servers are stored in the third tier of the Platform security layers. Servers are secured behind a firewall and cannot be directly reached from the public Internet.

7. **User Access Control.**

7.1. In connection with all GoodData Workspaces, only designated GoodData personnel, Company's administrators, or partner administrators can manage Customer access and remove from or manage Customer Data on the Platform. GoodData personnel can obtain user-level access to Customer Data only when explicitly invited by Company or a partner administrator for the purposes of technical support or when contractually authorized to provide professional services. The Platform supports role-based access control and user groups to define objects and capabilities within the Platform to which a Customer will have access..

7.2. There are additional measures that Company should use to implement Customer-specific access control policies.

7.2.1. IP whitelisting allows Company to define trusted IP address ranges from which Customers can

access Company's domains.

7.2.2. Custom session expiration allows Company to specify a period of inactivity after which sessions are terminated and Customers are automatically logged out of the Platform.

8. **Customer Data Privacy Controls.**

8.1. Customer Data is segregated into Workspaces (each corresponding to a single data mart) within a data warehouse instance. Customer access is managed on Workspace level to avoid any inappropriate access to Customer Data by unauthorized entities or individuals.

8.2. In addition, GoodData users are permitted access to Workspace data based on filters that designated administrators can define and apply to user accounts ("**Data Permissions**"). These Data Permission filters can be applied in order to restrict access of specific users to specific Workspace records and are applied to each user query submitted to the Workspace. For example, queries for a user can be restricted to a specific region or department. Implementation of Data Permissions must follow standard platform blueprints. Company acknowledges that Data Permissions are not designed as a mechanism for separation of user access across different legal entities, and Company remains responsible for Customer Data privacy oversight and compliance with respect to the Workspace activities undertaken by authorized Customers on the GoodData Platform.

9. **Data Security.**

9.1. **High Level Architecture**. The Platform architectural design is strategically arranged to promote Customer Data confidentiality, integrity and availability. This architecture includes:

- Data segregation;

- Consistency checks;

- Log management; and

- Active monitoring using situational awareness algorithms.

9.2. **Logical Task Separation**. Strict process separation is a built-in design feature of all GoodData software development and operational lifecycles. GoodData isolates and seals data and metadata in deployed multi-tenant security architectures, even while data and metadata shares the same physical storage grids. GoodData continuously monitors and performs situational awareness analysis that reveals data security anomalies and outliers for rapid response.

9.3. **Encryption**. Data transport and long-term storage are protected using industry standard methods of encryption (TLS, strong symmetric-key cryptography).

9.4. **Data Deletion and Disk Destruction**. GoodData maintains backups and archives of Customer Workspaces in line with its Data Backup Policy published on GoodData's website and updated from time to time. The backups are retained for a period of time that does not exceed ninety (90) days.

9.4.1. Company may request complete and permanent deletion of Customer Data (including off-site backups) by contacting GoodData Support.

9.4.2. The unit on which data destruction is applied is an entire Workspace. GoodData Support does

not perform Customer Data removal services on any lower granularity.

9.4.3. Upon the termination of Company's Subscription Services, GoodData shall make Customer Data available for retrieval for a period of thirty (30) days. Afterwards, GoodData will fully remove all Customer Data, including backups, within the next sixty (60) days.

9.4.4. GoodData's hosting service providers comply with industry standard secure media disposal standards and procedures.

9.5. **Malware/Virus Protection Procedure.** GoodData installs antivirus and anti-malware solutions with corporate policy settings and automated daily updates scheduled on all Microsoft® Windows® and Apple® Mac® OS X® based end-user workstations.

10. **Organizational Security and Change Management Processes**. GoodData deploys several operational access controls to help minimize the security risks associated with human activities. All GoodData employees with access to Customer Data undergo background checks, and access to the production environment is only permitted through a secure gateway using multi-factor authentication. Through the gateway, GoodData administrators may access Platform functions; but they are not permitted to directly interact with the Platform components. All privileged sessions are monitored and logged; logs are regularly reviewed by an independent security department.

11. **GoodData Access**.

11.1. **General System Access.** GoodData provides system access only to appropriately trained staff and requires a specific level of access to perform authorized tasks. Internal systems enforce unique user IDs and strong passwords and prohibit password reuse. To manage access, GoodData relies on industry-standard security systems and standards including LDAP, Kerberos, and RSA. Only authorized users can gain access to servers, logs, customer information, source code, installation packages and system configuration information.

11.2. **Production System Access**. Logical access to the production environment by GoodData employees is limited to authorized operational engineers only, protected by multi-factor authentication and allowed only when justified by a business need.

11.2.1. All access keys are stored within an encrypted credentials vault.

11.2.2. Access requests, grants and revocations are periodically reviewed.

11.2.3. All changes to access rights are based on GoodData personnel roles and their job responsibilities, and are subject to senior management oversight and approval. The approval process maintains audit records of all changes. The "least privilege" principle is applied and enforced.

11.2.4. Access to the production infrastructure servers for the Platform is restricted at the network level. Each server is accessible only from an access node, which in a segregated, "demilitarized zone" and which can be itself accessed only by authorized GoodData operations personnel including GoodData operations engineers. A specific set of credentials and assigned access rights is required for authentication from the access node; access to the access node server does not automatically

enable access to production servers.

11.2.5. A member of senior management monitors the revocation of access to employees who either become inactive or change job roles.

11.3. Other Access to Customer Data by GoodData. Authorized and trained GoodData personnel in the role of support or solution engineer may access Customer Data only under the following circumstances:

11.3.1. Based on Company's submitted “Support” request requiring use or access to Customer Data; Company shall provide Company's written consent for such requested access by GoodData;

11.3.2. When GoodData is authorized to provide “managed services” or is conducting a consulting services engagement under a statement of work.

11.4. Logs and Monitoring. All GoodData access to the Platform and Customer Data are recorded and logged, subject to regular access review by dedicated GoodData security personnel. GoodData log management practices comply with the applicable NIST recommendations and standards.

12. **Web Application Security Self-Assessment**. GoodData will regularly (with each release) undertake its own proactive internal web application security assessment incorporating OWASP methodology. GoodData will remediate any security risks arising from the outcome of the assessment in line with its committed SLAs.

13. **Incident Reporting and Response Process.** GoodData proactively monitors the Platform for security incidents, including alert notifications generated by GoodData systems and those of its infrastructure partners, open source and industry alerts and community alerts. When an alert is raised, the risk level is assessed first by internal GoodData personnel. Based on this assessment, the GoodData security team will select and launch the prescribed response process. Documented internal escalation procedures and communication protocols clarify when and how an internal escalation takes place, and who is notified. For events classified as an “**Incident**” (meaning an event impacting the Platform that triggers an alert and requiring prompt or immediate investigation by GoodData), GoodData personnel will respond to the incident within thirty (30) minutes from receipt of a triggered notice on a 24x7, 365 day, annual basis.

14. **Data Breach Notice Procedures**. GoodData will use all commercially reasonable efforts to notify Company in writing within seventy-two (72) hours after confirming or determining reasonable suspicion of an Incident involving unauthorized access to Customer Data, and will take all necessary steps and measures to promptly remediate any vulnerabilities involving Customer Data as soon as GoodData becomes aware of the security incident. Company must sign up and consent to receive security- and support-related emails from GoodData at the Online Support Portal.

15. **Continuous Improvement**. As the industry standards, regulations and technology evolve, GoodData will from time to time implement changes to improve its information security program. GoodData reserves the right to update or replace any of its information security practices, providing that such change (i) adequately addresses GoodData commitments outlined in this document and (ii) does not materially reduce the level of information security of the Platform.

16. **Applicability of this Annex II**. GoodData will make all commercially-reasonable efforts to ensure the information security of the Platform; however, to the extent that in the Agreement, a Statement of Work, or any

other agreement, Company requests or requires that GoodData modifies its standard practices in a way that is inconsistent with the terms of this Annex II, this Annex II will not apply. To the extent that Company implements changes to the Platform configuration which are inconsistent with the terms of this Annex II, this Annex II will not apply.

17. **Shared Responsibilities for Information Security**. GoodData's obligations under this Annex II apply solely to the extent that Company complies with its own responsibilities under the Agreement, including all applicable Statements of Work. Company acknowledges that it is responsible for ensuring the security of its own network, equipment, and Customers. Company understands the need to comprehensively assess risks related to its usage of the Platform and implement applicable security controls including complementary user entity controls to achieve a desired level of security. These complementary user entity controls include but are not limited to controls related to user access management, user security considerations such as endpoint protection, implementation of supplementary user access technical safeguards offered by GoodData such as SSO, IP whitelisting and custom session expiration, change management of Company's implementation, and notification to GoodData in case of a suspected or confirmed data security incident by sending email to security@gooddata.com, each of which will facilitate the achievement of Company's desired level of security.

18. **Additional Safeguards for Protection of Sensitive Personal Data**. If the Customer Data includes Sensitive Personal Data, GoodData will employ additional safeguards for protection of such Sensitive Personal Data. These safeguards are available under the Enterprise Shield package, which Company must purchase in order to be able to upload Sensitive Personal Data to the GoodData platform. The Enterprise Shield package employs more stringent logical access controls, formal assurance, and security review of the implementation, along with coverage of the implementation by SOC 2 Type II audit, and a complete audit trail of access to data by GoodData personnel and access to platform events audit log by Company. Sensitive Personal Data may not be shared via Scheduled E-mails and KPI Alerts.

PRODUCT: GOODDATA CLOUD - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. **Physical Access Controls**: the data importer shall take reasonable measures to prevent physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorized persons from gaining access to personal data.

2. **System Access Controls**: the data importer shall take reasonable measures to prevent personal data from being used without authorization. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access

on several levels.

3. **Data Access Controls**: the data importer shall take reasonable measures to provide that personal data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the personal data to which they have privilege of access; and, that personal data cannot be read, copied, modified or removed without authorization in the course of processing. In addition to the access control rules set forth in Sections 1-3 above, data importer implements an access policy under which access to its system environment, to personal data and other data by authorized personnel only.

4. **Transmission Controls**: the data importer shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of personal data by means of data transmission facilities is envisaged so personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. **Input Controls**: the data importer shall take reasonable measures to provide that it is possible to check and establish whether and by whom personal data has been entered into data processing systems, modified or removed. Data importer shall take reasonable measures to ensure that (i) the personal data source is under the control of data exporter; and (ii) personal data integrated into data importer's systems is managed by secured file transfer from the data importer and data subject.

6. **Data Backup**: the data importer shall ensure that back-ups are taken on a regular basis, are secured, and encrypted when storing personal data to protect against accidental destruction or loss when hosted by data importer.

7. **Logical Separation**: the data importer shall ensure that data from the data exporter is logically segregated on the data importer's systems to ensure that personal data that is collected for different purposes may be processed separately.

8. **Shared Responsibilities for Information Security:** Company agrees that in accordance with Applicable Data Protection Law and before submitting any Personal Data to the Services, Company will perform an appropriate risk assessment to determine whether the security measures within the Services provide an adequate level of security, taking into account the nature, scope, context and purposes of the processing, the risks associated with the Personal Data and the Applicable Data Protection Laws. GoodData will provide Company reasonable assistance by providing Company with information requested by Company to conduct Company's security risk assessment. Company is solely responsible for determining the adequacy of the security measures within the Services in relation to the Personal Data Processed. Sensitive Personal Data may not be shared via Scheduled E-mails and KPI Alerts.