DATA PROCESSING AGREEMENT 数据处理协议

This Data Processing Agreement ("DPA") reflects the parties' agreement with respect to the terms governing the Processing of Personal Data on behalf of the Customer under any applicable written agreement between Customer and Dynatrace governing the use of the Dynatrace Offerings (paid or otherwise), and any related order forms, attachments, and statements of work (collectively, the "Agreement"). To the extent the parties have not executed a separate Data Processing Agreement, this DPA will become effective as of the date the Dynatrace Offerings start as listed in the applicable Order Form.

本数据处理协议（"DPA"）反映了根据以下各方就代表客户管理个人数据处理的条款达成一致：客户与 Dynatrace 之间关于使用 Dynatrace 产品和服务（付费型或其他）的任何适用书面协议，以及任何相关的订购单、附件和工作说明书（这些文件统称为"协议"）。如果双方尚未签署单独的数据处理协议，则本 DPA 将自相关订单中列出的 Dynatrace 产品开始提供之日起生效。

This DPA is subject to the terms of, and fully incorporated and made part of, the Agreement. This DPA shall replace any existing data processing agreement unless otherwise explicitly stated herein. In the event of any conflict between this DPA and any other provision of the Agreement with respect to personal data, this DPA shall govern and apply. Capitalized terms used but not defined in this DPA have the same meanings as set out in the Subscription Agreement available at https://cdn.dm.dynatrace.com/assets/documents/legal/Data-Processing-Agreement-Chinese-Simplified-2025-01-07.pdf

本 DPA 受协议条款的约束，且完全纳入协议并成为协议的一部分。本 DPA 取代任何现有的数据处理协议，除非本 DPA 中另有明确注明。如果本 DPA 与协议中有关个人数据的任何其他规定有任何冲突，应以本 DPA 为准。本 DPA 中使用但未专门定义的大写术语与《认购协议》中规定的含义相同。《认购协议》载于 https://cdn.dm.dynatrace.com/assets/documents/legal/Data-Processing-Agreement-Chinese-Simplified-2025-01-07.pdf

1. Definitions. 定义

   (a) "APPI" means the Japanese Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2016).
   "APPI"是指日本《个人信息保护法》(2003 年第 57 号法案，2016 年修订）。

   (b) "Data Protection Law" means all data protection and data privacy laws and regulations applicable to Dynatrace's Processing of Customer Personal Data under the Agreement.
   "数据保护法律"是指适用于 Dynatrace 根据协议处理客户个人数据的所有数据保护、数据隐私法律法规。

   (c) "Controller" has the same meaning given under the applicable Data Protection Law and includes "Database Owner" under the Protection of Privacy Law of Israel and "Business" under the applicable US State Privacy Law.
   "控制方"与适用的数据保护法律规定的含义相同，其包括以色列《隐私保护法》规定的"数据库所有者 "和适用的美国州立隐私法规定的"企业"。

   (d) "Customer Personal Data" means any Personal Data submitted, stored, posted, displayed, or otherwise transmitted by or on behalf of Customer in the course of using the Dynatrace Offerings; and excludes Personal Data (such as Restricted Information) submitted, stored, posted, displayed, or otherwise transmitted by or on behalf of Customer in violation of any provision of the Agreement and/or this DPA.

“客户个人数据”是指在使用 Dynatrace 产品和服务的过程中由客户或其他方代表客户提交、存储、发布、展示或以其他方式传输的任何个人数据，但不包括以有违协议和或本 DPA 的方式由客户或其他方代表客户提交、存储、发布、展示或以其他方式传输的任何个人数据（例如“受限信息”）。

(e) “Dynatrace Group” means one or more of Dynatrace LLC, a Delaware limited liability company, and its Affiliates that may assist Dynatrace to provide the Dynatrace Offerings, and/or related support or services, under the Agreement and this DPA.
“Dynatrace 集团”是指特拉华州有限责任公司 Dynatrace LLC 及其关联方（它们可能协助 Dynatrace 提供协议和本 DPA 项下的 Dynatrace 产品和服务、和/或相关支持或服务）中的一家或多家。

(f) “Europe” means the European Union, European Economic Area (“EEA”), and/or their member states, Switzerland, and the United Kingdom.
“欧洲”是指欧盟、欧洲经济区（“EEA”）和/或两者的成员国、瑞士和英国。

(g) “GDPR” means the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
“GDPR”是指欧洲议会和理事会关于在个人数据处理和此类数据自由流动方面保护自然人的第 2016/679 号条例（《通用数据保护条例》）。

(h) “LGPD” means the Lei Geral de Proteção de Dados Pessoais (General Personal Data Protection Act in Brazil).
“LGPD”是指“Lei Geral de Proteção de Dados Pessoais”（巴西《通用数据保护法》）。

(i) “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Personal Data while being transmitted, stored, or otherwise Processed by Dynatrace.
“个人数据泄露”是指在 Dynatrace 传输、存储或以其他方式处理客户个人数据时发生的安全泄漏，导致客户个人数据遭到意外或非法破坏、丢失、篡改、或未经授权的披露或访问。

(j) “PIPL” means the China Personal Information Protection Law.
“PIPL”是指中国《个人信息保护法》。

(k) “Personal Data” means “Personal Data,” or “Personal Information” as defined under applicable Data Protection Laws that Dynatrace collects or receives on behalf of Customer. Personal Data does not include information that Dynatrace obtains or Processes independent of the performance of its respective obligations under the Agreement with Customer.
“个人数据”是指 Dynatrace 代表客户收集或接收的适用数据保护法律定义的“个人数据”或“个人信息”。个人数据不包括 Dynatrace 在与履行与客户签订的协议项下各自义务无关的过程中获取或处理的信息。

(l) “Processor” has the same meaning given under the applicable Data Protection Law and includes “Holder” as defined under the Protection of Privacy Law of Israel, and “Service Provider” under the applicable US State Privacy Law.
“处理方”与适用的数据保护法律规定的含义相同，其包括以色列《隐私保护法》规定的“持有人”和适用的美国州立隐私法规定的“服务提供商”。

(m) “Standard Contractual Clauses” means the Standard Contractual Clauses promulgated by the EU Commission Decision 2021/914/EU incorporated herein by reference as updated amended or replaced from time to time.
“标准合约条款”是指欧盟委员会第 2021/914/EU 号决议颁布的标准合约条款（以不时更新、修订或替换的为准），通过引用而纳入本 DPA。

(n) “Sub-processor” means Processors engaged by Dynatrace or members of the Dynatrace Group to enable Dynatrace to deliver/provide the Dynatrace Offerings under the terms of the Agreement or this DPA.
“分处理方”是指由 Dynatrace 或 Dynatrace 集团旗下成员聘请的处理方，其目的是使 Dynatrace 能够根据协议或本 DPA 的条款交付/提供 Dynatrace 产品和服务。

(o) “Supervisory Authority” means the government agency, department, or other competent organization with authority over the processing of Personal Data relevant to this DPA.
“监督机构”是指有权监督与本 DPA 相关的个人数据处理的政府机构、部门或其他主管组织。

(p) “UK Addendum” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner’s office under S119A (1) Data Protection Act 2018, attached hereto as Schedule D, as updated, amended or replaced from time to time.
“英国增补”是指由英国信息专员办公室根据 2018 年《数据保护法》第 S119A(1) 条颁布的《欧盟委员会标准合约条款数据跨境传输附件》（以不时更新、修订或替换的为准），作为附录 D 附于本 DPA。

(q) “Business”, "Controller", “Consumer,” "Processor," “Service Provider,” "Data Subject", “Sell,” “Supervisory Authority”, and "Processing" (and "process") shall have the meanings given under applicable Data Protection Law.
“企业”、“控制方”、“消费者”、“处理方”、“服务提供商”、“数据主体”、“出售”、”和“处理”具有适用的数据保护法律所赋予的含义。

2. Applicability of DPA and Parties’ Roles
DPA 的适用性和各方的角色

(a) This DPA applies to Processing of Customer Personal Data by Dynatrace on behalf of the Customer to perform its obligations and exercise its rights under the Agreement and this DPA. For the avoidance of doubt this DPA does not apply to Processing of Customer Personal Data by Dynatrace as a Controller.
本 DPA 适用于 Dynatrace 出于履行其在协议和本 DPA 下之义务和行使其在协议和本 DPA 下之权利的目的而代表客户处理客户个人数据。为避免疑义，本 DPA 不适用于 Dynatrace 作为控制方对客户个人数据的处理。

(b) Customer is a Controller or a Processor and Dynatrace is a Processor. To the extent applicable under Data Protection Law, Customer appoints Dynatrace as a Processor to process the Customer Personal Data on Customer's behalf.
客户是控制方或处理方，Dynatrace 是处理方。在数据保护法律的适用范围内，客户指定 Dynatrace 为处理方，以代表客户处理客户个人数据。

3. Processing of Customer Personal Data 客户个人数据的处理

(a) The nature and extent of Processing Customer Personal Data by Dynatrace to deliver the Dynatrace Offerings is determined and controlled by Customer and is supplemented by Schedule A. The nature, purpose and duration of the Processing, as well as the types of Personal Data collected and categories of Data Subjects whose Personal Data may be Processed by Dynatrace, are described in Schedule A to this DPA. Customer acknowledges that Dynatrace does not have any knowledge of the actual data or types of Personal Data contained in the Customer Data. The parties agree that the Customer's complete and final instructions about the nature and purposes of the Processing in connection with the Dynatrace
Offerings are set out in the Agreement and this DPA.
Dynatrace 为交付 Dynatrace 产品和服务而处理客户个人数据的性质和范围由客户决定和控制，详见附录 A 中予以补充说明。本 DPA 的附录 A 描述了个人数据处理的性质、目的和持续时间，以及所收集个人数据的类型和数据主体的类别。客户承认，Dynatrace 对客户数据中所含个人数据的实际数据或类型不知情。双方同意，客户关于与 Dynatrace 产品和服务相关的处理的性质和目的的最终完整指示载于协议和本 DPA 中。

(b) Any changes or modifications to the instructions shall be communicated in writing and acknowledged by both parties. Dynatrace shall inform Customer if, in its reasonable opinion, Customer's processing instructions are likely to infringe any applicable Data Protection Law; in such event, Dynatrace is entitled to refuse Processing of Customer Personal Data that it believes to be in violation of any applicable Data Protection Law until Customer amends its instruction so as not to be infringing.
对这些指示的任何更改或修改均应以书面形式通知，并由双方确认方为有效。如果 Dynatrace 合理认为客户的数据处理指示可能违反任何适用的数据保护法律，则应通知客户；在这种情况下，Dynatrace 有权拒绝进行其认为违反任何适用数据保护法律的客户个人数据处理，直到客户修改其指示至不再违法。

(c) To the extent Customer's configuration of Dynatrace Offerings results in Dynatrace capturing Customer Personal Data, Customer represents and warrants that, it will, at all times, comply with all applicable Data Protection Law. As between Customer and Dynatrace, Customer is responsible for: (i) protecting Customer Personal Data while using Dynatrace by configuring Dynatrace Data Privacy Settings as described at https://docs.dynatrace.com/docs/manage/data-privacy-and-security (Dynatrace instructions on how to configure data privacy settings) to granularly control the scope of Customer Personal Data to be captured by the Dynatrace Offerings; (ii) the accuracy, quality and legality of Customer Personal Data, and the means by which Customer or any relevant third-party acquired Personal Data.
在客户对 Dynatrace 产品和服务的配置导致 Dynatrace 捕获客户个人数据的情况下，客户声明并保证其将始终遵守所有适用的数据保护法律。在客户和 Dynatrace 之间， 客户应负责：(i) 在使用 Dynatrace 时通过配置 Dynatrace 数据隐私设置来保护客户个人数据，详情参见 https://docs.dynatrace.com/docs/manage/data-privacy-and-security（Dynatrace 有关如何配置数据隐私设置的操作说明），以对 Dynatrace 产品和服务捕获客户个人数据的范围进行精细控制；(ii) 客户个人数据的准确性、质量和合法性，以及客户或任何相关第三方获取个人数据的方式。

(d) If Customer is a processor acting on behalf of a third-party Controller, Customer warrants to Dynatrace that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Dynatrace as another Processor, have been authorized by the relevant Controller.
如果客户是代表第三方控制方行事的处理方，则客户向 Dynatrace 保证，客户就该客户个人数据的指示和行动（包括其将 Dynatrace 指定为另一处理方），已获得相应控制方的授权。

(e) Customer represents and warrants that: (i) it will inform its Data Subjects as legally required about its use of Processors to Process their Customer Personal Data, including Dynatrace, including where required providing notice

to Data Subjects about the use of the Dynatrace Offerings; (ii) it has obtained, and continues to have, during the term, all necessary rights, lawful basis, authorizations, and/or valid consent from Data Subjects for the Processing of Customer Personal Data by Dynatrace as contemplated by the Agreement; (iii) Dynatrace's Processing of Customer Personal Data in accordance with the Agreement will not violate applicable Data Protection Laws or cause a breach of any agreement or obligations between Customer and any third party.
客户声明并保证：(i) 客户将按照法律要求，向数据主体告知其使用处理方（包括 Dynatrace）处理客户个人数据的情况，包括在需要时向数据主体提供有关使用 Dynatrace 产品和服务的通知；(ii) 对于 Dynatrace 按照协议设想处理客户个人数据，客户已在协议期限内继续拥有所有必要的权利、合法依据、授权和/或有效同意；(iii) 客户对 Dynatrace 产品和服务的使用不会，并且不会导致 Dynatrace，违反任何数据保护法律或其他适用的法律法规，或客户与任何第三方之间的任何协议或义。

(f) Customer will provide Dynatrace only with the Customer Personal Data necessary for Dynatrace to perform its obligations under the Agreement with respect to the Dynatrace Offerings and any related services. Customer acknowledges that the use of the Dynatrace Offerings does not require and is not suitable for the Processing of any Restricted Information and will not, through its use of the Dynatrace Offerings, provide any Restricted Information to be Processed by Dynatrace.
客户将仅向 Dynatrace 提供必要的客户个人数据，以便 Dynatrace 履行其在协议项下有关 Dynatrace 产品和任何相关服务的义务。客户承认，使用 Dynatrace 产品和服务不需要也不适合处理任何受限信息，并且不会通过使用 Dynatrace 产品和服务提供任何受限信息给 Dynatrace 处理。

4. Requests from Third Parties. 第三方的请求。

(a) Dynatrace Offerings provide Customer with functionality to access Customer Personal Data in order to assist Customers with requests from Data Subjects exercising their rights granted to them under Data Protection Law ("Data Subject Requests") or requests from regulatory or judicial bodies relating to the Processing of Customer Personal Data. To the extent that Customer is unable to access the relevant Customer Personal Data within Dynatrace Offerings or the access to Customer Personal Data does not provide sufficient assistance to answer such requests in accordance with Data Protection Law, and where required by applicable Data Protection Law, Dynatrace agrees, at the Customer's request, to provide reasonable assistance to Customer, to enable Customer to respond to Data Subject Requests or requests from regulatory or judicial bodies relating to the Processing of Customer Personal Data under the Agreement. If a request is made directly to Dynatrace relating to Customer Personal Data for which Dynatrace can identify Customer as the Controller, Dynatrace shall without undue delay refer such communication to Customer and shall not respond to such request without Customer' express authorization. The foregoing shall not prohibit Dynatrace from communicating with a Data Subject or regulatory or judicial body if it is not reasonably apparent on the face of the communication that the request relates to the Customer or if Dynatrace has a legal obligation to respond itself.
Dynatrace 产品和服务为客户提供了访问客户个人数据的功能，在数据主体根据数据保护法律行使权利而提出请求（"数据主体请求"）或监管或司法机构提出与客户个人数据处理有关的要求的情况下，这些功能可以协助客户履行回应义务。如果客户无法访问 Dynatrace 产品和服务中的相关客户个人数据，或者访问客户个人数据无法提供足够的帮助来满足根据数据保护法律提出的此类请求，并且根据适用数据保护法律的要求，Dynatrace 同意应客户请求向客户提供合理的帮助，使客户能够就协议项下的客户个人数据处理回应数据主体请求或监管或司法机构提出的请求。如果是 Dynatrace 可识别为控制方的客户直接向 Dynatrace 提出与客户个人数据相关的请求，Dynatrace 应及时将此类通信转达给客户，不得无故拖延，并且未经客户明确

授权不得回应此类请求。如果从通信内容中无法合理判断该请求与客户有关，或者 Dynatrace 有法律义务自行回应，则上述条文并不禁止 Dynatrace 与数据主体或监管或司法机构进行沟通

。

(b) If Dynatrace is compelled to disclose Personal Data for which Customer is the Controller due to a request by a law enforcement agency or other third-party, Dynatrace will give Customer notice of such request before granting access and/or providing Personal Data, to allow Customer to seek a protective order or other appropriate remedy. If Dynatrace is legally prohibited from providing Customer notice, Dynatrace will take measures to protect Personal Data from undue disclosure, as if it were Dynatrace's own Confidential Information being requested.
如果 Dynatrace 因执法机构或其他第三方的要求而被迫披露客户作为控制方的个人数据，Dynatrace 将在允许访问和/或提供个人数据之前通知客户，以便客户寻求保护令或其他适当的补救。如果法律禁止 Dynatrace 向客户发出此类通知，Dynatrace 将采取措施保护个人数据不被不当披露，就像对待 Dynatrace 自己的机密信息一样。

5. Assistance and Cooperation. Subject to the nature of the processing and the Personal Data available to Dynatrace and where required by applicable Data Protection Law, Dynatrace will, upon Customer's written request, provide reasonable assistance and information to Customer, where, in Customer's judgement, the type of Processing performed by Dynatrace requires a data protection impact assessment, and/or prior consultation with the relevant data protection authorities and provide reasonable assistance to Customer in complying with its other obligations under applicable Data Protection Law relating to data security and Personal Data Breach notifications, to the extent applicable to the Processing of Customer Personal Data. Customer shall reimburse Dynatrace for all non-negligible costs Dynatrace incurs in performing its obligations under this section.
协助与合作。根据处理的性质和 Dynatrace 可获得的个人数据，以及适用数据保护法律的要求，Dynatrace 将应客户的书面请求，在客户判断 Dynatrace 执行的处理类型需要进行数据保护影响评估和/或事先咨询相关数据保护机构的情况下，向客户提供合理的协助和信息；并在适用于客户个人数据处理的范围内，向客户提供合理的协助，以便其遵守适用数据保护法律规定的与数据安全和个人数据泄露通知相关的其他义务。客户应向 Dynatrace 补偿 Dynatrace 在履行本节规定的义务所产生的所有非可忽略的费用。

6. Demonstrable Compliance. Dynatrace agrees to provide information necessary to demonstrate compliance with this DPA upon Customer's reasonable request. 可证明的合规性。Dynatrace 同意，在客户合理请求下，将提供必要信息，以证明遵守本 DPA。

7. Audits and Assessments. 审计和评估。

(a) Where applicable Data Protection Laws afford Customer an audit or assessment right and subject to the scope of such right, Customer may carry out, upon Customer's written request and up to once per year, an audit or assessment of Dynatrace's policies, procedures, and records relevant to the Processing of Customer Personal Data, in accordance with applicable Data Protection Laws. 在适用的数据保护法律赋予客户审计或评估权并且属于此类权利范围内的情况下，客户可在提出书面请求的情况下，根据适用的数据保护法律，对与客户个人数据处理相关的 Dynatrace 政策、程序和记录进行审计或评估，每年最多一次。

(b) To request an audit, Customer must submit a detailed audit plan at least four (4) weeks in advance of the proposed audit date to Dynatrace, which plan describes the proposed scope, duration, and start date of the audit. Dynatrace will review the audit plan and provide Customer with any concerns or questions. Before the commencement of any audit, the parties shall agree on a detailed audit plan, including fees, timing, scope of controls, evidence to be produced, and

duration. If the requested audit scope is addressed in a similar audit report within the prior twelve months and Dynatrace confirm there are no material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.
要请求进行审计 ，客户必须在提议的审计日期前至少提前四 (4) 周向 Dynatrace 提交一份详细的审计计划，说明提议的审计范围、持续时间和开始日期。Dynatrace 将审查审计计划，并向客户提出任何疑虑或问题。在开始任何审计之前，双方应就详细的审计计划达成一致，包括费用、时间、控制范围、要出示的证据和持续时间。如果所请求的审计范围在之前 12 个月内的类似审计报告中已有涉及，且 Dynatrace 确认所审计的控制措施没有重大变更，则客户同意接受其审计结果，放弃请求对报告中涉及的控制措施进行审计。

(c) Any audit or assessment must be: (i) conducted during Dynatrace's normal business hours; (ii) subject to the parties' confidentiality obligations. If a third-party is to conduct the audit, the third-party must not be a competitor to Dynatrace, and such third-party is subject to Dynatrace's prior consent, and must execute a written confidentiality agreement with the parties before conducting the audit.
任何审计或评估必须：(i) 在 Dynatrace 正常营业时间内进行；(ii) 遵守双方的保密义务。如果由第三方进行审计，该第三方不得是 Dynatrace 的竞争对手，且该第三方须事先征得 Dynatrace 的同意，并在进行审计前与双方签署书面保密协议。

(d) Any audits are at Customer's expense. Any request for Dynatrace to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from, or in addition to, those required for the provision of the Dynatrace Offerings. Dynatrace will seek Customer's written confirmation that it will pay any applicable fees before performing such audit assistance.
所有审计费用均由客户承担。如果请求 Dynatrace 协助审计需要使用不同于提供 Dynatrace 产品和服务所需的资源，或在提供 Dynatrace 产品和服务所需资源之外使用的其他资源，则该请求将被视为一项单独的服务。Dynatrace 将要求客户书面确认其将在进行此类审计协助之前支付任何适用费用。

8. Confidentiality. Dynatrace shall ensure that any person that it authorizes to process the Customer Personal Data (including its staff, agents, and subcontractors) shall be subject to a contractual, statutory duty, or other binding obligations of confidentiality.
保密性。Dynatrace 应确保其授权处理客户个人数据的任何人员（包括其员工、代理和分包商）应遵守合同、法定职责或其他具有约束力的保密义务。

9. Security 安全规定

(a) Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Dynatrace has implemented and shall maintain appropriate technical and organizational measures designed to provide a level of security appropriate to the risk of Processing Customer Personal Data ("Security Measures"). Customer confirms that Dynatrace's implementation of the Security Measures identified at Schedule B is sufficient for the purposes of complying with its obligations under this DPA. Notwithstanding the above, Customer acknowledges and agrees it is responsible for its own secure use of the Dynatrace Offerings.
安全措施。考虑到处理的现有技术、实施成本、性质、范围、背景和目的，以及自然人权利和自由的不同可能性和不同严重程度的风险，Dynatrace 已实施并应维持适当的技术性和组织性措施，以提供与处理客户个人数据的风险级别相匹配的安全水准（"安全措施"）。客户确认，Dynatrace 实施的安全措施（列于附录 B ）足

以满足其在本 DPA 项下的义务。尽管有上述规定，客户承认并同意，其对自己安全使用 Dynatrace 产品和服务负责。

(b) Personal Data Breach. Dynatrace will notify Customer without undue delay and no later than required of Dynatrace by applicable Data Protection Law, after it becomes aware of a Personal Data Breach.
Dynatrace will promptly initiate an investigation into the circumstances surrounding the Personal Data Breach and make its findings available to Customer. Dynatrace will endeavour to take all steps required by applicable Data Protection Law to mitigate the effects of such Personal Data Breach. At Customer's request and taking into account the nature of the Processing and information available to Dynatrace, Dynatrace will take commercially reasonable steps to assist Customer in complying with its obligations necessary to enable Customer to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Customer is required to do so under applicable Data Protection Law. Notification of a Personal Data Breach will be delivered to one or more of Customer's administrators by any means Dynatrace selects including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the online portal or as otherwise required by Dynatrace in a written notice to Customer's administrator(s). Dynatrace's obligation to report or respond to a Personal Data Breach under this Section is not an acknowledgement by Dynatrace of any fault or liability with respect to the Personal Data Breach.
个人数据泄露。在 Dynatrace 获悉发生个人数据泄露后，Dynatrace 不得无故拖延且以不迟于适用数据保护法律要求的时限通知客户。Dynatrace 应立即对围绕个人数据泄露的情况展开调查，并将调查结果提供给客户。Dynatrace 将尽力采取适用数据保护法律要求的所有措施，减轻此类个人数据泄露的影响。应客户的请求，并考虑到处理的性质和 Dynatrace 可获得的信息，Dynatrace 在履行必要义务的过程中，应采取商业上合理的行动来协助客户，使客户能够将相关个人数据泄露通知主管机构和/或受影响的数据主体（如果适用的数据保护法律要求客户这样做）。个人数据泄露的通知将通过 Dynatrace 选择的任何方式（包括通过电子邮件）发送给客户的一位或多位管理员。客户应自行负责确保客户的管理员在门户网站上或者按照 Dynatrace 给客户管理员的书面通知中的另行要求，保留准确的联系信息。Dynatrace 根据本条规定对个人数据泄露进行报告或响应的义务并不构成 Dynatrace 承认与个人数据泄露有关的任何过失或责任。

10. Sub-processing 分处理

(a) Customer gives its general authorization to appoint members of the Dynatrace Group as sub-processors under this DPA and authorizes Dynatrace and members of the Dynatrace Group to engage further Subprocessors. A current list of current Sub-processors for the Dynatrace Offerings is available at https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/. To be notified of new Sub-processors or changes in Sub-processors, Customer must register for notifications available at https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatraceservices/ ("Data Protection Notices"). Dynatrace shall update the Sub-processor List to reflect any addition or change in third-party Sub-processors not less than thirty (30) days prior to the effective date of the change. Customers that have subscribed to get updates to the Sub-processor List will be notified of the change.
客户授予一项一般授权，指定 Dynatrace 集团旗下成员作为本 DPA 项下的分处理方，并允许 Dynatrace 和 Dynatrace 集团旗下成员聘用进一步的分处理方。Dynatrace 产品和服务的当前分处理方的最新名单（"分处理方名单"）载于 https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/。若要获得新的分处理方或分处理方变更的通知，客户必须在

https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/（“数据保护通知”）上注册，以获取此类通知。Dynatrace 应在分处理方变更生效前至少提前三十 (30) 天更新分处理方名单，以反映第三方分处理方的任何新增或变更。订阅了分处理方名单更新的客户将收到此类变更的通知。

(b) To the extent required by applicable Data Protection Law, Customer may object to the processing of Customer Personal Data by any newly appointed Sub-processor on reasonable grounds relating to the protection of Customer Personal Data and shall inform Dynatrace in writing within fifteen (15) days after notice of the changes are posted on the Sub-processor List, setting out the specific reasons for its objection. Customer's objection must be in writing and provide commercially reasonably justification for the objection, based on reasonable concerns concerning the proposed Sub-processor's practices relating to data protection. Following an objection, the parties will then work together in good faith to address Customer's reasonable objections and proceed with the change in Sub-processor. If an agreement cannot be reached within fifteen (15) days of the objection, at Dynatrace's option: (a) Dynatrace will instruct the Sub-processor not to process Customer Personal Data, which may result in a Dynatrace Offerings feature being suspended and unavailable to Customer, or (b) Customer may immediately terminate this DPA and the Agreement and Dynatrace will promptly refund a prorated portion of any prepaid fees for the period after such suspension or termination date. If no objection is received by Dynatrace within the time period specified above, Customer shall be deemed to have approved the use of the new sub-processor.
在适用数据保护法律要求的范围内，如果客户基于合理理由反对由任何新指定分处理方处理客户个人数据，则应在 Dynatrace 在分处理方名单上发布变更后十五（15）天内以书面形式通知 Dynatrace，说明其反对的具体原因。客户的反对意见必须以书面形式提出，并提供商业上合理的反对理由，这些理由应基于对拟定的分处理方在数据保护方面的做法的合理担忧。提出异议后，双方应真诚合作，以解决客户的合理反对意见，并进行分处理方的更换。如果双方无法在提出反对意见后十五（15）天内就客户的反对意见达成一致，则 Dynatrace 应自行抉择以下两种解决办法之一：(a) Dynatrace 将指示分处理方不要处理客户个人数据，这可能导致 Dynatrace 产品和服务功能被暂停而客户无法使用；(b) 允许客户立即终止本 DPA 和协议，并且 Dynatrace 将及时按比例退还已预付的此类暂停或终止日期之后时间段的任何费用。如果 Dynatrace 在上述规定的期限内未收到任何反对意见，则应被视为客户已批准使用新的分处理方。

(c) Dynatrace shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide substantially similar appropriate contractual obligations but not less restrictive than those set forth in this DPA, to the extent appropriate to the nature of the service provided by such Subprocessor; and (ii) remain responsible for such Sub-processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-processor that cause Dynatrace to breach any of its obligations under this DPA.
Dynatrace 应：(i) 与每个分处理方签订书面协议，其中包含数据保护义务，在该分处理方提供的服务性质适用的范围内，提供的合同义务与本 DPA 中规定的义务基本类似，但限制性不得低于本 DPA 中的规定；(ii) 仍然对该分处理方遵守本 DPA 的义务以及该分处理方导致 Dynatrace 违反其在本 DPA 项下任何义务的任何作为或不作为承担责任。

11. Deletion of Customer Data on Termination. Following termination or expiry of the Agreement Customer Personal Data will be deleted within thirty (30) days, or, at the choice of customer, returned, except as required to be retained by applicable law or to the extent archived on back-up systems, in which case the terms of this DPA shall survive.

终止时客户数据的删除。协议终止或到期后，客户个人数据将在三十 (30) 天内删除，或按照客户的选择退回，但适用法律要求保留的数据或备份系统存档的数据除外，在此情况下，本 DPA 条款继续有效。

12. International Data Transfers 数据跨境传输

(a) Customer authorizes Dynatrace and its Sub-processors to transfer Customer Personal Data across international borders, including without limitation from the EEA, UK, and/or Switzerland, Israel, and China to the United States. If Customer Personal Data originating from the EEA or Switzerland is transferred to a country that has not been found to provide an adequate level of protection under applicable Data Protection Law ("Restricted Transfer"), the parties agree that the transfer shall be governed by the Standard Contractual Clauses that are hereby incorporated by reference into this DPA as follows. The signatures on this DPA or the Agreement constitute signing the Standard Contractual Clauses and any annexes attached thereto. When the transfer of Customer Personal Data from Customer ("Data Exporter") to Dynatrace ("Data Importer") is a Restricted Transfer and Data Protection Laws require that a valid transfer mechanism be put in place, the transfers shall be subject to the Standard Contractual Clauses.
客户授权 Dynatrace 及其分处理方跨境传输客户个人数据，包括但不限于从欧洲经济区、英国、瑞士、以色列、中国传输到美国。如将源于欧洲经济区或瑞士的客户个人数据传输到一个无法根据适用数据保护法律提供足够保护水准的国家（"受限传输"），双方同意，此类传输受标准合约条款规管，标准合约条款在此通过引用而纳入本 DPA。在本 DPA 或协议上的签名构成对标准合约条款及其随附任何附件的签署。如从客户（"数据导出方"）向 Dynatrace（"数据导入方"）传输的客户个人数据属于受限传输且数据保护法律要求建立有效的传输机制，则此类传输应遵守标准合约条款。

(b) The Standard Contractual Clauses shall be completed as follows: 标准合约条款应补充如下内容：

i. Module Two will apply (as applicable); 模块 2 将适用（如适用）；

ii. In Clause 7 (Docking), the optional docking clause will apply; 在第 7 条（对接）中，可选的对接条款将适用；

iii. In Clause 8.5 and Clause 16 (d), the certification of deletion will be provided upon data exporter's written request;
在第 8.5 条和第 16(d) 条中，应数据导出方的书面请求，将提供删除证明；

iv. In Clause 8.9, the audit right shall be carried out in accordance with Section 7 of the DPA; 在第 8.9 条中，应根据 DPA 第 7 条执行审计权；

v. In Clause 9 (Use of Sub-processors), option 2 "General Written Authorization" for subprocessors shall apply and the time period for prior notice shall be as set out in section 11 of this DPA;
在第 9 条（分处理方的使用）中，选项 2 针对分处理方的"一般书面授权"条款应适用，且事先通知的时间期限应如本 DPA 第 11 条所述；

vi. In Clause 11 (Redress), the optional language shall not apply; 在第 11 条（救济）中，可选语言不适用；

vii. In Clause 13 (Supervision), the competent supervisory authority shall be the Commission nationale de l'informatique et des libertes (CNIL). 在第 13 条（监督）中，主管监督机构应为法国国家信息与自由委员会 (CNIL)。

viii. In Clause 14 (f) and Clause 16 (c), the termination right will be limited to the termination of the Clauses;

在第 14(f) 条和第 16(c) 条中，终止权仅限于终止相应条款；

ix. In Clause 17 (Governing Law), the Standard Contractual Clauses shall be governed by French law; 在第 17 条（管辖法律）中，标准合约条款应受法国法律管辖；

x. In Clause 18(b) (Choice of Forum and Jurisdiction), the parties agree that disputes shall be resolved before the courts of France;
在第 18(b) 条（诉讼地和管辖权的选择）中，双方同意争议应提交法国法院裁决；

xi. Annex 1 of the Standard Contractual Clauses shall be completed with the information set out in Schedule A of this DPA;
标准合约条款的附件一应补充本 DPA 的附录 A 中载明的信息；

xii. Annex 2 of the Standard Contractual Clauses shall be completed with the information set out in Schedule B of this DPA; and
标准合约条款的附件二应补充本 DPA 的附录 B 中载明的信息；以及

xiii. A new Clause 1 (e) is added to the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the parties' Processing of Customer Personal Data that is subject to the Swiss Federal Act on Data Protection. Where applicable, reference to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to the transfer of Customer Personal Data that are subject to the Swiss Federal Act on Data Protection and the Swiss Federal Data Protection and Information Commissioner as the supervisory authority under these Clauses.". 标准合约条款新增第 1 (e) 条，内容如下："在本文适用范围内，这些条款经适当变通后也适用于受瑞士联邦《数据保护法》约束的各方对客户个人数据的处理。在适用的情况下，对欧盟成员国法律或欧盟监管机构的引用应进行修改，以包括瑞士法律下的适当引用，因为它涉及受瑞士联邦《数据保护法》管辖的客户个人数据的传输，以及瑞士联邦数据保护和信息专员作为本条款下的监管机构。"

(c) To the extent Dynatrace's provision of the Dynatrace Offerings involves the transfer of Customer Personal Data originated from the UK to a third country that has not been designated as providing an adequate level of protection for Customer Personal Data under the Applicable Laws in the UK, the Standard Contractual Clauses shall: (i) be used and completed as set forth in section 13; (ii) a new Clause 1(f) is added to the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses, as supplemented by Section 13, also apply mutatis mutandis to the parties' Processing of Customer Personal Data that is subject to the UK Data Protection Laws; and (iii) the UK Addendum shall be completed as follows:
如果 Dynatrace 提供的 Dynatrace 产品和服务涉及将源于英国的客户个人数据传输到未被英国适用法律认定为对客户个人数据提供足够保护的第三国，则 (i) 应使用标准合约条款并补充第 13 条的内容；(ii) 在标准合同条款中添加新的第 1(f) 条，内容如下(i) 按照第 13 条的规定使用和填写；(ii) 标准合约条款新增第 1 (e) 条，内容如下："在本文适用范围内，经第 13 条补充的这些条款经适当变通后也适用于各方对受英国数据保护法律管辖的客户个人数据的处理；(iii) 《英国增补》应补充如下内容：

i. Table 1 of the UK Addendum shall be completed with the information in Schedule A.
《英国增补》的表 1 应补充附录 A 中的信息。

ii. Table 2 of the UK Addendum shall be completed with the information located in Section 13 (c) of this DPA.
《英国增补》的表 2 应补充本 DPA 第 13(c) 条中的信息。

iii. Table 3 of the UK Addendum shall be completed as follows:

《英国增补》的表 3 应补充如下内容：

1) The list of parties is set forth in Schedule A; 各方的名单载于附录 A；

2) A description of the transfer is set forth in Schedule A; 有关传输的描述载于附录 A；

3) A description of the technical and organizational measures is set forth in Schedule B; 有关技术性和组织性措施的描述载于附录 B；

4) The list of sub-processors is in section 11 of this DPA; 分处理方名单载于本 DPA 第 11 条；

5) For purposes of completing Table 4 of the UK Addendum, both the importer and the exporter may end the UK Addendum as set out in Section 19 of the UK Addendum. 就填写《英国增补》表 4 而言，导入方和导出方均可按照《英国增补》第 19 条的规定终止《英国增补》。

(d) To the extent Dynatrace's provision of the Dynatrace Offerings involves the transfer of Customer Personal Data originated from China to a third country that has not been designated as providing an adequate level of protection for Customer Personal Data under the Applicable Laws in China), Customer shall be responsible for fulfilling all the following obligations for exporting Customer Personal Data (where Customer is the Controller) or ensuring that all the following obligations have been fulfilled by the relevant third-party controller (where Customer is the Processor):
如果 Dynatrace 提供的 Dynatrace 产品和服务涉及将源于中国的客户个人数据传输到未被中国适用法律认定为对客户个人数据提供足够保护的第三国，则客户应负责履行以下有关出口客户个人数据的所有义务（在客户为控制方的情况下），或确保相关第三方控制方已履行以下所有义务（在客户为处理方的情况下）：

i. informing the individuals of the name and contact information of the overseas receiving party of Customer Personal Data, the purpose and means of the Processing, the categories of Customer Personal Data, and the methods and procedures via which the individuals may raise requests to exercise the rights to Customer Personal Data with the overseas receiving party of Customer Personal Data;
告知客户个人数据海外接收方的个人名称和联系信息、处理目的和方式、客户个人数据的类别，以及个人就行使客户个人数据权利向客户个人数据海外接收方提出要求的方法和程序；

ii. securing a lawful basis for the export of Customer Personal Data, and where consent of the individuals is the lawful basis, obtaining separate consent of the individuals;
确保出口客户个人数据的合法依据，如果合法依据是个人同意，则应征得个人的单独同意；

iii. conducting a personal information protection impact assessment on the exporting of Customer Personal Data; and
对客户个人数据的出口进行个人信息保护影响评估；以及

iv. adopting the appropriate safeguard measure required by the PIPL and accompanying administrative regulations (i.e., passing the government security assessment, filing the executed standard contractual clauses or obtaining the certification) unless exemption applies.
采取《个人数据保护法》(PIPL) 和相关行政法规要求的适当保障措施（例如，通过政府安全评估、提交已执行的标准合约条款或获得认证），除非适用豁免。

(e) In addition to the foregoing, if a Supervisory Authority adopts, updates or replaces any standard contractual clauses or similar data transfer mechanisms, Dynatrace reserves the right to adopt an alternative compliance standard to replace or supplement the Standard Contractual Clauses or the UK Addendum for the lawful transfer of Personal Data, or add

new data transfer mechanisms for other countries, provided these are recognized under Data Protection Law. Dynatrace will provide thirty (30) days advance notice of the adoption of the alternative compliance standard to customers who subscribe to Data Protection Notices. The variation will automatically apply as set out in Dynatrace's notification at the end of the notice period. 除上述规定外，如果监督机构采用、更新或取代任何标准合约条款或类似的数据传输机制，Dynatrace 保留采用替代性合规标准以取代或补充《标准合约条款》或《英国增补》的权利，以便合法传输个人数据，或针对其他国家增加新的数据传输机制，前提是这些机制得到数据保护法律的认可。Dynatrace 将提前三十 (30) 天向订阅数据保护通知的客户提供采用替代性合规标准的通知。在通知期结束时，此类变更将自动按照
Dynatrace 通知中载明的规定适用。

(f) In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the Standard Contractual Clauses (provided however, Processor may appoint Sub-processors as set out, and subject to the requirements of, Section 11 of this DPA) or a similar mechanism required by applicable Data Protection Laws specifically for international data transfers; (2) this DPA; and (3) the Agreement.
如果以下文件之间有任何冲突或不一致，其优先顺序为：(1) 标准合约条款（但处理方可按照本 DPA 第 11 条的规定和要求指定分处理方）或适用数据保护法律专门针对数据跨境传输所要求的类似机制；(2) 本 DPA ；(3) 协议。

(g) To the extent Dynatrace transfers Customer Data originating from and protected by applicable Data Protection Law in Brazil, Dynatrace shall comply with the principles and rights of Data Subjects and the data protection obligations provided in the LGPD.
如果 Dynatrace 传输的客户数据源自巴西并受适用的巴西数据保护法律保护，Dynatrace 应遵守 LGPD 中规定的数据主体的原则和权利，并遵守其中规定的数据保护义务。

(h) To the extent Dynatrace transfers Customer Data originating from and protected by applicable Data Protection Law in Japan, Dynatrace shall comply with the principles and rights of Data Subjects and the data protection obligations provided in the APPI.
如果 Dynatrace 传输的客户数据源自日本并受适用的日本数据保护法律保护，Dynatrace 应遵守 APPI 中规定的数据主体的原则和权利，并遵守其中规定的数据保护义务。

(i) To the extent Dynatrace's provision of the Dynatrace Offerings involves the transfer of Customer Personal Data originated from Israel to a third country that has not been designated as providing an adequate level of protection for Customer Personal Data under the Applicable Laws in Israel), Customer shall be responsible for securing a lawful basis for the export of Customer Personal Data. For clarity, this DPA constitute as Dynatrace's written obligation for adopting the appropriate safeguard measures required by the Protection
of Privacy Regulations (International Data Transfer), 2001. For the sake of clarity, the obligations in this DPA are deemed sufficient by the Customer to facilitate the transfer of information outside the Israel in accordance with Regulation 3 of the Privacy Protection Regulations (Transfer of Data to Databases Outside the Borders of the Country), 2001.
如果 Dynatrace 提供的 Dynatrace 产品和服务涉及将源自以色列的客户个人数据传输到未被以色列适用法律认定为对客户个人数据提供足够保护的第三国，则客户应负责确保客户个人数据出口的合法依据。为明确起见，本 DPA 构成 Dynatrace 采取 2001 年《隐私保护条例（数据跨境传输）》所要求的适当保障措施的书面义务。为明确起见，客户认同本 DPA 中的义务足以促进根据 2001 年《隐私保护条例》第 3 条（向境外数据库传输数据）将信息传输到以色列境外。

13. Supplemental US State Privacy Laws Specific Terms. 美国州立隐私法补充特定条款。

(a) The definition of "Applicable Data Protection Law" includes US State Privacy Laws. "US State Privacy Laws" means all state laws relating to the protection and processing of personal data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.
"适用数据保护法律"的定义包括美国州立隐私法。"美国州立隐私法"是指在美国生效的与个人数据保护和处理相关的所有州立法律，其中可能包括但不限于经《加利福尼亚州隐私权法》("CCPA") 修订的《加利福尼亚州消费者隐私法》以及其他州的类似消费者隐私法，在每种情况下，均可能会不时进行修订、补充或替代.

(a) Where Dynatrace processes Customer Personal Data subject to US State Privacy Laws, Dynatrace is a "service provider" or "processor" (as applicable) when processing Customer Personal data. Customer discloses, or otherwise makes available, Customer Personal Data to Dynatrace for a limited and specified purpose of providing Dynatrace Offerings in accordance with the Agreement (the "Purpose"). Dynatrace shall (and will require that its Sub-processors):
在 Dynatrace 根据美国州隐私法处理客户个人数据的情况下，Dynatrace 在处理客户个人数据时是服务提供商或（如适用）处理方。客户向 Dynatrace 披露或以其他方式提供客户个人数据的目的，仅限于按照本协议提供本协议中所述的 Dynatrace
产品和服务（以下简称"目的"）。Dynatrace 应（并将要求其分处理方）：

i. comply with obligations applicable to it as a service provider or processor under US State Privacy Laws ;
遵守美国州隐私法规定的适用于其作为服务提供商或（如适用）处理方的义务；

ii. notify if it can no longer meet its obligations under US State Privacy Laws ;
如果无法继续履行 美国州隐私法规定的义务，则应发出通知；

iii. not "sell" or "share" (as such terms are defined by the CCPA) Customer Content or retain, use, or disclose Customer Personal Data: (1) for any purpose other than the Purpose, including retaining, using, or disclosing Customer Personal Data for a commercial purpose other than the Purpose, or as otherwise permitted by US State Privacy Laws; or (2) outside of the direct business relationship between Customer and Dynatrace; or, unless otherwise permitted by US State Privacy Laws , not combine Customer Personal Data with Personal Data that Dynatrace receives from or on behalf of another business or person, or that it collects from its own interactions with individuals, unless such combination is required to perform any business purpose as permitted by US State Privacy Laws.
在一些情况下，不出售或分享（这些术语的定义见 CCPA）客户内容，不保留、使用或披露客户个人数据：(1) 出于"目的"之外的
任何目的，包括出于"目的"或美国州隐私法允许的其他目的之外的商业目的而保留、使用或披露客户个人
数据；或 (2) 在客户和 Dynatrace 之间的直接业务关系之外；或者，除非美国州隐私法允许，否则不得将
客户个人数据与 Dynatrace 从其他企业或个人或代表其他企业或个人收到的个人数据或 Dynatrace 从其自身与个人的互动中收集的个人数据进行合并，除非此类合并是为了实现美国州隐私法（包括

其任何

条例）或加利福尼亚州隐私保护机构通过的法规所允许的任何商业目的。

iv. Customer will: (1) upon notice, have the right to take reasonable and appropriate steps agreed upon by the parties to help ensure that Dynatrace Processes Customer Personal Data in a manner consistent with Customer's obligations under US State Privacy Laws and to stop and remediate unauthorized Processing of Customer Personal Data by Dynatrace Processing of Customer Personal Data by Dynatrace; (2) notify Customer if it makes a determination that it can no longer meet its obligations under US State Privacy Laws in relation to Customer Personal Data
客户将：(1) 在收到通知后，有权采取双方同意的合理且适当的措施，帮助确保 Dynatrace 以符合美国州隐私法规定的客户义务的方式处理客户个人数据，并停止和补救 Dynatrace 未经授权处理客户个人
数据的行为；(2) 如果 Dynatrace 确定其无法再履行 美国州隐私法规定的作为服务提供商的义务，且该等义务与客户个人数据相关，则将通
知客户。

v. Dynatrace acknowledges and confirms that it does not receive Customer Personal Data as consideration for any Offerings provided to Customer. Dynatrace certifies that it understands and will comply with its obligations under US State Privacy Laws.
Dynatrace 承认并确认，其不会将接收客户个人数据作为向客户提供任何产品和服务的对价。
Dynatrace 证明其理解并将遵守美国州隐私法规定的义务。

5 Miscellaneous 其他规定

(a) Except as amended by this DPA, the Agreement will remain in full force and effect. Any amendments to this DPA shall be in writing duly signed by authorized representatives of the parties.

(a) 除经本 DPA 修订外，协议应保持完全效力。对本 DPA 的任何修订均应以书面形式进行，并由双方授权代表正式签署方为有效。

(b) Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, any order or the Agreement, whether in contract, tort or under any other theory of liability, shall remain subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA, including all Schedules hereto. Dynatrace shall not be liable to Customer for indirect or consequential loss or damage, loss of profit, loss of sales, loss of business, loss of anticipated savings, loss of or damage to goodwill, or otherwise in each case whether direct or indirect which arise out of or in connection with this DPA. Without limiting either of the parties' obligations under the Agreement or this DPA, Customer agrees that any liability incurred by Dynatrace in relation to the Customer Personal Data that arises as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or applicable Data Protection Law shall count toward and reduce Dynatrace's liability limit under the Agreement (or if applicable, under this DPA) as if it were liability to the Customer. Notwithstanding anything to the contrary in this DPA (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.
尽管协议或本 DPA 中有任何相反的规定，每一方及其所有关联方因本 DPA、协议或任何订单引起的或与之相关的责任，在合约、民事侵权行为或任何其他责任原则方面，按总体累计仍应遵守协议的"责任限额"章节。在该章节中对一方责任的任何提及均是指该方及其所有关联方在协议和本 DPA （包括所有附录）项下的总责任。Dynatrace 对客户因协议引起的或与协议有关的间接或后果性的损失或损害、利润损失、

销售损失、业务损失、预期费用节省的损失、商誉损失或损害、或其他任何情况下的直接或间接损失或损害概不承担责任。在不限制任何一方在协议或本 DPA 项下义务的情况下，客户同意，如果因客户未能遵守其在本 DPA 或适用数据保护法律项下的义务或与之相关而为 Dynatrace 招致与客户个人数据相关的任何责任，应计入并相应减少 Dynatrace 在协议项下（或如果适用，在本 DPA 项下）的责任限额，就如同此类责任是客户的责任。无论本 DPA 中是否有任何相反规定（包括但不限于任何一方的赔偿义务），对于监管机构或政府机构根据 GDPR 第 83 条对一方开出或征收的与其违反 GDPR 相关的 GDPR 罚金，另一方均不承担责任。

(c) This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement provided that the Standard Contractual Clauses will be governed as set out in section 13 of this DPA.
本 DPA 应受协议中所述管辖法律和管辖权规定的管辖，并据其进行解释，前提是标准合约条款的管辖将按本 DPA 第 13 条的规定。

SCHEDULE A 附录
A

DETAILS OF THE PROCESSING 处理详情

Description of Data Exporter
数据导出方说明

The data exporter is the entity identified as the "Customer" or "Dynatrace", as the case may be in case of any Sub-processing, in the Data Processing Agreement in place between data exporter and data importer and to which this Schedule is appended.
数据导出方是指在数据导出方与数据导入方签订的《数据处理协议》（本附录附于该协议之后）中被确认为"客户"或"Dynatrace"的实体（在任何分处理中视情况而定）。

Description of Data Importer
数据导入方说明

The data importer is the entity identified as "Dynatrace" or a duly authorized Sub-processor in the Data Processing Agreement in place between data exporter and data importer and to which this schedule is appended.
数据导入方是在数据导出方与数据导入方签订的《数据处理协议》（此附录附于该协议之后）中被确认为"Dynatrace"或经正式授权的分处理方的实体。

Subject Matter and Duration of the Processing
处理的标的物和持续时间

The subject-matter and duration of the processing is as follows:
处理的标的物和持续时间如下：

As between the parties, Customer shall be the Controller of certain Customer Personal Data provided to Dynatrace by Customer in connection to its use of Dynatrace Offerings. The duration of the processing shall be the term of the Agreement.
就缔约双方而言，对于由客户提供给 Dynatrace 的，与使用 Dynatrace 产品和服务相关的某些客户个人数据，客户应为控制方。处理的持续时间应为协议的有效期限。

Purposes of the Processing
处理的目的

The processing is necessary for the following purposes: 出于以下目的需要进行处理：

To enable Dynatrace to provide the Dynatrace Offerings to Customer and exercise its rights and obligations under the Agreement. 使 Dynatrace 能够向客户提供 Dynatrace 产品和服务并行使其在协议项下的权利和义务。

Data Subjects
数据主体

The data subjects may include: (i) users authorized by the Customer to use the Dynatrace Offerings and (ii) users of or visitors to Customer's monitored applications and/or websites (including but not limited to the Customer's employees, customers or clients, agents, contractors, and advisors) as determined in the Customer's sole discretion.

数据主体可能包括：(i) 获得客户授权而使用 Dynatrace 产品和服务的用户；(ii) 客户的受监控应用程序和/或网站的用户或访问者（包括但不限于客户的雇员、客户或顾客、代理人、承包商和顾问），此类用户或访问者的身份由客户自行认定。

Type of Personal Data

个人数据类型

Customer is required to provide certain Personal Data in order to use the Dynatrace Offerings, including IP address and first and last name if included in a user's e-mail address and user credentials. Customer may submit additional Personal Data to the Dynatrace Offerings, the extent of which is determined and controlled by Customer in its sole discretion.

客户需要提供某些个人数据以使用 Dynatrace 产品和服务，包括 IP 地址以及姓名（如果后者包含在用户的电子邮件地址和用户登录凭据中）。客户可能会向 Dynatrace 产品和服务提交额外的个人数据，其范围由客户自行决定和管控。

Special categories of data or sensitive personal data (if appropriate)

特殊类别的数据和敏感个人数据（如适用）

The Personal Data transferred concern the following special categories of data or sensitive personal data:

传输的个人数据涉及以下特殊类别的数据和敏感个人数据：

Not applicable. Customer may not use the Dynatrace Offerings to process any data classified as "special category data" or "sensitive personal data" unless explicitly agreed in writing.

不适用。除明确书面同意外，客户不得使用 Dynatrace 产品和服务处理归类为"特殊类别数据"或"敏感个人数据"的任何数据。

Processing Operations

处理操作

The personal data transferred will be subject to the following basic processing activities:

传输的个人数据应限于以下基本处理活动：

Dynatrace shall process the Customer Personal Data only as necessary to provide the Dynatrace Offerings and exercise its rights and obligations as contained in the terms of the Agreement and this Data Processing Agreement, including but not limited to customer enablement, technical support, professional services, improving Dynatrace Offerings performance and functions, user authentication and communications and account administration.

Dynatrace 应仅在提供 Dynatrace 产品和服务和行使协议和本 DPA 条款所载的权利和义务所必需的情况下处理客户个人数据，此类情况包括但不限于客户支持、技术支持、专业服务、改进 Dynatrace 产品和服务性能和功能、用户身份验证、用户通信以及账户管理。

SCHEDULE B 附录
B

SECURITY MEASURES 安全措施

Dynatrace (also referred to herein as the "Processor"), will implement, at least, the technical and organizational security measures described below in respect of the Customer Personal Data it Processes on behalf of the Customer (also referred to herein as the "Controller"). These security measures shall be applied to all Customer
Personal Data that is subject to the underlying agreement between the Processor and the Controller (the "Agreement"). In relation to third party sub-processors that may process Personal Data on Dynatrace's behalf, such third party will have its own security requirements to protect the Personal Data.
Dynatrace（本附录中也称为"处理方"）将针对其代表客户（本附录中也称为"控制方"）处理的客户个人数据至少实施以下技术性和组织性安全措施。这些安全措施应适用于受处理方与控制方所签基础协议（"协议"）管辖的所有客户个人数据。对于可能代表 Dynatrace 处理个人数据的第三方分处理方，该第三方应有自身的安全要求来保护个人数据。

Technical measures 技术性措施

1.1 Authorization 授权

(a) An authorization system shall be used where different authorization profiles are used for different purposes. 当不同的授权配置文件被用于不同的目的时，应使用授权系统。

1.2 Identification 身份识别

(a) Every Authorized User must be issued with a personal and unique identification code for that purpose ("User ID"). A User ID may not be assigned to another person, even at a subsequent time.
每个授权用户都必须为该目的取得唯一的个人识别代码（"用户 ID"）。同一用户 ID 不得分配给其他人，即使是在随后的时间也应如此。

(b) An up-to-date record shall be kept of Authorized Users, and the authorized access available to each, and identification and authentication procedures shall be established for all access to information systems or for carrying out any Processing of Data. As used herein, "Processing" refers to any operation or set of operations which is performed on Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
应保留授权用户的最新记录。对于所有对信息系统的访问或执行任何数据处理，应建立为每个用户提供授权访问以及身份识别和验证的程序。本附录中使用的术语"处理"是指对数据执行的任何一项操作或一组操作，无论是否通过自动化方式进行，例如收集、记录、组织、结构化、存储、改编或更改、检索、查阅、使用、通过传输披露、传播或以其他方式提供、排列或组合、限制、删除或销毁。

(c) Passwords shall be modified periodically as set forth in the Information Security Policies. 密码应根据《信息安全政策》的规定定期修改。

1.3 Authentication 身份验证

(a) Authorized Users shall be allowed to Process Data if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific Processing operation or to a set of Processing operations.
如果授权用户获得了身份验证凭证，例如成功完成与某项具体处理操作或一组处理操作相关的身份验证程序，则应允许其处理数据。

(b) Authentication must be based on a secret password associated with User ID, and which password shall only be known to the Authorized User. 身份验证必须基于与用户 ID 相关联的密码，该密码只有授权用户知晓。

(c) One or more authentication credentials shall be assigned to, or associated with, an Authorized User. 一个或多个身份验证凭证应分配给授权用户或与授权用户相关联。

(d) There must be a procedure for password confidentiality and integrity. Passwords must be stored in a way that makes them unintelligible while they remain valid. There must be a procedure for assigning, distributing and storing passwords.
必须建立维持密码保密性和完整性的程序。密码的存储方式必须使其在有效期内难以破解。必须建立密码分配、分发和存储的程序。

(e) Passwords shall consist of at least twelve characters, or, if this is not technically permitted by the relevant information systems, a password shall consist of the maximum permitted number of characters. Passwords shall not contain any item that can be easily related to the Authorized User in charge of the Processing and must be changed at regular intervals, which intervals must be set out in the security document. Passwords shall be modified by the Authorized User to a secret value known only to the Authorized User when it is first used and periodically thereafter. 密码应至少由十二个字符组成；或者，如因受相关信息系统限制在技术上不允许，则密码应由最多允许数量的字符组成。密码不得包含任何容易与负责处理的授权用户相关联的字符项，并且必须按一定的时间间隔定期更改，该间隔必须在安全文件中载明。密码应由授权用户修改成秘密值，该秘密值在首次使用以及此后使用时应仅限该授权用户知晓。

(f) In addition to a valid user ID and password combination, all access to Dynatrace data or systems must be secured by a Multi-Factor Authentication ("MFA") solution. The MFA solution can be either software or hardware in nature.
除了有效的用户 ID 和密码组合外，对 Dynatrace 数据或系统的所有访问都必须通过多因素身份验证 ("MFA") 解决方案进行保护。MFA 解决方案可以是软件，也可以是硬件。

(g) Authentication credentials shall be also de-activated if the Authorized User is terminated or transferred or de- authorized from accessing the information systems or Processing Data.
如果授权用户被终止、转移或取消访问信息系统或处理数据的授权，其身份验证凭证也应被停用。

1.4 Access controls 访问控制

(a) Only Authorized Users shall have access to Data, including when stored on any electronic or portable media or when transmitted. Authorized Users shall have authorized access only to those data and resources necessary for them to perform their duties.
只有授权用户才能访问数据，包括存储在任何电子或便携式介质上或传输时。授权用户应仅有权限访问各自履行职责所必需的数据和资源。

(b) A system for granting Authorized Users access to designated data and resources shall be used. 应使用一个系统来授予授权用户访问指定数据和资源的权限。

(c) It shall be verified semi-annually, that the prerequisites for retaining the relevant authorization profiles still apply. This may also include the list of Authorized Users drawn up by homogeneous categories of task and corresponding authorization profile.
相关授权配置文件的先决条件应每半年经过一次核验，确保其仍然适用。这也可能包括基于同类任务类别和相应的授权配置文件制定的授权用户列表。

(d) Measures shall be put in place to prevent a user gaining unauthorized access to, or use of, the information systems. In particular, intrusion detection systems reflecting industry best practice should be installed to protect the information systems from unauthorized access.
应制定相关措施，防止用户未经授权访问或使用信息系统。特别是，应安装符合行业最佳实践的入侵检测系统，以保护信息系统免受未经授权的访问。

(e) Operating system or database access controls must be correctly configured to ensure authorized access only. 必须正确配置操作系统或数据库访问控制，以确保只有获得授权的人员方可访问。

(f) Only those staff authorized shall be able to grant, alter or cancel access by users to the information systems. 只有获得授权的员工才能授予、更改或取消用户对信息系统的访问权限。

1.5 Management of computer systems and removable media 计算机系统和可移动介质的管理

(a) Network information systems and physical media storing Data must be housed in a secure environment with physical access restricted to staff that are authorized to have such access. Strong authorization and access controls must be maintained.
网络信息系统和存储数据的物理介质必须存放在安全环境中，其物理访问仅限于获得此类授权访问的员工。必须保持强力的授权和访问控制。

(b) The software, firmware and hardware used in the information systems shall be reviewed annually in order to detect vulnerabilities and flaws in the information systems and resolve such vulnerabilities and flaws.
信息系统中使用的软件、固件和硬件应每年进行一次审查，以发现信息系统中的漏洞和缺陷并加以解决。

(c) Policies and training shall be issued with regard to keeping and using media on which Data are stored in order to prevent unauthorized access and Processing. 应发布和开展有关保存和使用数据存储介质的政策和培训，以防止未经授权的访问和处理。

(d) When media are to be disposed of or reused, necessary measures shall be taken to prevent any subsequent retrieval of the Data and other information previously stored on them, or to otherwise make the information intelligible or be re-constructed by any technical means before they are withdrawn from the inventory. All reusable media used for the storage of Data will be overwritten a minimum of three times with randomized data prior to disposal or re-use.

对介质进行处置或者再利用时，应当采取必要措施，防止先前存储的数据和其他信息以后被恢复，或者以其他方式通过任何技术手段使此类信息变得可理解或重新构建，之后方可从库存中提取。用于存储数据的所有可重复使用的介质，在处置或重复使用之前，应采用随机数据覆盖至少三遍。

(e) The removal of media containing Data from the designated premises must be specifically authorized by the Controller and in compliance with Dynatrace policies. 从指定场所移除含有数据的介质，必须得到控制方的特别授权并遵守 Dynatrace 的相关政策。

(f) Media containing Data must be erased or rendered unreadable if it is no longer used and prior to proper disposal. 如果含有数据的介质不再使用，在妥善处置之前，必须擦除数据或使其不可读。

1.6 Distribution or transmission 分配或传输

(a) Data must only be available to Authorized Users. 仅限向授权用户提供数据。

(b) Encryption (128-bit or stronger) or another equivalent form of protection must be used to protect Data that is electronically transmitted over a public network or stored on a portable device, or where there is a requirement to store or Process Data in a physically insecure environment.
如果以电子方式通过公共网络传输数据或数据存储在便携式设备中，或者需要在不安全的物理环境中存储或处理数据，必须采用加密（128 位或以上）或其他等效保护形式来保护数据。

(c) When Data are to leave the designated premises as a result of maintenance operations, the necessary measures shall be taken to prevent any unauthorized retrieval of the Data and other information stored therein.
当数据因维护操作而将要离开指定场所时，应采取必要措施，防止数据和存储在其中的其他信息被未经授权检索。

(d) Where Data is transmitted or transferred over an electronic communications network, measures shall be put in place to control the flow of data and record the timing of the transmission or transfer, the Data transmitted or transferred, the destination of any Data transmitted or transferred, and details of the Authorized User conducting the transmission or transfer.
如果通过电子通信网络传输或传送数据，则应制定措施控制数据流动，并记录传输或传送的时间、传输或传送的数据、任何数据传输或传送的目的地，以及进行传输或传送的授权用户的详细信息。

1.7 Preservation, back-up copies and recovery 保存、备份副本和恢复

(a) Procedures must be defined and laid down for making back-up copies and for recovering Data. These procedures must provide for Data to be reconstructed in the state they were in at the time they were lost or destroyed.
必须制定和落实制作备份副本和恢复数据的程序。这些程序必须确保在发生数据丢失或时，数据能重建为备份时的状态。

(b) Back-up copies must be made at least once a week, unless no Data have been updated during that period.
必须至少每周制作一次备份副本，除非在此期间没有更新数据。

(c) A back-up copy and data recovery procedures must be kept at a different location from the site of the information systems Processing the Data and these minimum security requirements shall apply to such back- up copies.
备份副本和数据恢复程序必须保存在与处理数据的信息系统站点不同的位置，这些最低安全要求适用于此类备份副本。

1.8 Anti-virus and intrusion detection 防病毒和入侵检测

(a) Anti-virus software and intrusion detection systems should be installed on the information systems to protect against attacks or other unauthorized acts in respect of information systems. Antivirus software and intrusion detection systems should be updated regularly in accordance with the industry best practice for the information systems concerned (and at least annually).
所有信息系统应安装防病毒软件和入侵检测系统，以防止信息系统受到攻击或其他未经授权的行为。应按照相关信息系统的行业最佳实践定期更新（每年至少更新一次）防病毒软件和入侵检测系统。

1.9 Testing 测试

(a) Testing prior to the implementation or modification of the information systems Processing Data shall not use real or 'live' data unless such use is necessary and there is no reasonable alternative. Where real or 'live' data is used, it shall be limited to the extent necessary for the purposes of testing and the level of security corresponding to the type of Data Processed must be guaranteed.
在实施或修改处理数据的信息系统之前进行的测试中，不得使用真实或"实时"数据，除非此类使用是必需的且没有合理的替代数据。在使用真实或"实时"数据的情况下，应将其限定在测试目的所需的范围内，并且必须针对所处理的数据类型保证达到相对应的安全级别。

1.10 Audit 审计

(a) Regular audits of compliance with these security requirements, at least annually, should be performed.
应定期对是否符合这些安全要求的合规性进行审计，每年至少一次。

(b) The results must provide an opinion on the extent to which the security measures and controls adopted comply with these security requirements, identify any shortcomings and (if any) propose corrective or supplementary measures as necessary. It should also include the data, facts and observations on which the opinions reached, and the recommendations proposed.
审计结果必须就所采用的安全措施和控制措施符合这些安全要求的程度提供意见，查明任何缺陷（如有）并提出必要的纠正或补充措施。审计结果还应包括得出意见所依据的数据、事实和观察所见，以及提出的建议。

2. Organizational measures 组织性措施

2.1 Security plan and document 安全计划和文件

- The measures adopted to comply with these security requirements shall be the subject of the Company's Information Security Policies and set out in a security portal, which shall be kept up to date, and revised whenever relevant changes are made to the information system(s) or to technical or organizational measures.
  为遵守这些安全要求而采取的措施应是公司信息安全政策的主题，其应在在安全门户网站中载明，该门户网站应保持最新，并在对信息系统、技术性或组织性措施进行更改时进行相应修订。

- The Information Security Policies shall address: 信息安全政策应涵盖以下方面：

  (i) Security measures relating to the modification and maintenance of the system(s) used to Process Data, including development and maintenance of applications, appropriate vendor support and an inventory of hardware and software;
  与修改和维护用于处理数据的系统相关的安全措施，包括应用程序的开发和维护、适当的供应商支持，以及硬件和软件库存；

  (ii) Physical security, including security of the buildings or premises where Data Processing occurs, security of data equipment and telecommunication infrastructure and environmental controls; and
  物理安全，包括进行数据处理的建筑物或场所的安全、数据设备和电信基础设施的安全，以及周边环境控制措施；和

  (iii) Security of computers and telecommunication systems including procedures for managing back-up copies, procedures dealing with computer viruses, procedures for managing signal/codes, security for software implementation, security related to databases, security for connecting systems to the Internet, inspection of circumvention of data system(s), mechanisms for keeping account of attempts to break system security or gain unauthorized access.
  计算机和电信系统的安全，包括管理备份副本的程序、处理计算机病毒的程序、管理信号/代码的程序、软件实施的安全、与数据库相关的安全、将系统连接到互联网的安全性、检查数据系统规避，记录试图破坏系统安全或获得未经授权访问的机制。

- The security plan shall include all Dynatrace policies, as updated from time to time, including but not limited to:
  安全计划应包含 Dynatrace 不时更新的所有政策，包括但不限于：

  (i) Code of Business Conduct and Ethics 商业行为规范和道德准则

  (ii) Global Data Protection Policy 全球数据保护政策

  (iii) Dynatrace IT Acceptable Use Policy
  Dynatrace 信息技术可接受使用政策

  (iv) System Security Policies: Dynatrace Access Control Management Policy; Backup Retention Standard; Change Management Policy; Change Management Policy - Business Systems; Compliance Policy ; Cyber and Data Security Incident Response Plan; Data Classification Policy; Data Loss Prevention Policy; Electronic Monitoring Policy; Encryption Policy; Human Resources Security Policy; Information Resource Management Policy; Information Risk Management Policy; IT Operations Policy; Mobile Device Policy; Network Access Policy; Network Account Password Policy; Network Firewall Policy; Physical Security &

Environmental Policy; Returning of Assets for Terminated Employees Policy; Secure; Security Phishing Policy; Service Account Lifecycle Policy; Vendor Management Policy; Vulnerability Management Policy; Workstation Security Policy.
系统安全政策：Dynatrace 访问控制管理政策；备份保留标准；变更管理政策；变更管理政策 - 业务系统；合规政策；网络和数据安全事件响应计划；数据分类政策；数据丢失预防政策；电子监控政策；加密政策；人力资源安全政策；信息资源管理政策； 信息风险管理政策；IT 运营政策；移动设备政策；网络访问政策；网络账户密码政策；网络防火墙政策；物理安全与环境政策；离职员工资产归还政策；网络钓鱼安全政策；服务账户生命周期政策；供应商管理政策；漏洞管理政策；工作站安全政策。

(v) The security plan shall be available to staff who have access to Data and the information systems, and must cover the following aspects at a minimum:
安全计划应提供给有权限访问数据和信息系统的员工，并且必须至少涵盖以下方面：

(vi) The scope, with a detailed specification of protected resources; 适用范围，其中详细阐述受保护的资源；

(vii) The measures, standards, procedures, code of conduct rules and norms to guarantee security, including the control, inspection and supervision of the information systems;
保障安全的各项措施、标准、程序、行为准则、规则和规范，包括对信息系统的控制、检查和监督；

(viii) The procedures for reporting, managing and responding to incidents; and 事件报告、管理和响应程序；以及

(ix) The procedures for making back-up copies and recovering Data including the member of staff who undertook the Processing activity, the Data restored and, as appropriate, which data had to be input manually in the recovery process.
制作备份副本和恢复数据的程序，包括承担处理活动的员工、恢复的数据以及在恢复过程中必须手动输入的数据（视情况而定）。

2.2 Functions and obligations of staff 员工的职能和义务

- Only members of staff that have a legitimate operational need to access the information systems or carry out any Processing of Data shall be authorized to do so (“Authorized Users”).
只有对访问信息系统或进行任何数据处理具有合法操作需求的员工方可被授权进行此类访问或处理（“授权用户”）。

- The necessary measures shall be adopted to train and make staff familiar with these minimumsecurity requirements, any relevant policies and applicable laws concerning the performance of their functions and duties in respect of the Processing of Data and the consequences of any breach of these requirements.
应采取必要措施对员工进行培训，使员工熟悉这些最低安全要求、与数据处理方面需要履行的职能和职责有关的任何相关政策以及适用法律，并了解违反这些要求的后果。

- The functions and obligations of staff having access to Data and the information systems shall be clearly defined through application security roles. 应通过应用程序安全角色，明确界定有权限访问数据和信息系统的员工的职能和义务。
- Authorized Users shall be instructed to the effect that electronic equipment should not be left unattended or made accessible during Processing sessions. Physical access to areas where any Data is stored shall be restricted to Authorized Users. The disciplinary measures for a breach of the security plan shall be clearly defined and documented and communicated to staff. 应指示授权用户在处理期间不得让电子设备处于无人看管或可擅自访问的状态。对数据存储区域的物理访问仅限于授权用户。应明确界定对违反安全计划的纪律处分，形成文件并传达给员工。

2.3 Chief Security Officer 首席安全官

- A person or persons responsible for the overall compliance with these minimum-security requirements shall be designated as the Chief Information Security Officer ("CISO"). The CISO shall be suitably trained and experienced in managing information security and provided with appropriate resources to effectively ensure compliance.
  应指定一人或多人担任首席信息安全官（"CISO"），负责全面遵守这些最低安全要求。 CISO 应在管理信息安全方面接受过适当的培训且具备经验，并获取适当的资源以有效确保合规。
- The contact details of the CISO shall be provided to the Controller upon request. 当控制方提出请求时，应将 CISO 的联系方式提供给控制方。

2.4 Record keeping 记录保存

- A history of Authorized User access to, or disclosure of, Data shall be recorded with a secure audit trail. 应与安全审计跟踪一并记录授权用户访问或披露数据的历史。
- Only those staff duly authorized may have physical access to the premises where information systems and media storing Data are stored. 只有经过正式授权的员工才能对存储信息系统和数据存储介质的场所进行物理访问。
- There shall be a procedure for reporting, responding to and managing security incidents such as data security breaches. This shall include at a minimum:
  应制定安全事件（例如数据安全违规行为）的报告、响应和管理程序。这至少应包括：
  (i) A procedure for reporting such incidents/breaches to appropriate management; 向适当管理层报告此类事件/违规行为的程序；
  (ii) A clearly designated team for managing and coordinating the response to an incident led by the CISO;
  一个明确指定的团队，负责在 CISO 领导下管理和协调事件响应；
  (iii) A documented process for managing the response to an incident including the requirement to keep appropriate issues and action logs to include the time at which the incident occurred, the person reporting the incident, to whom it was reported and the effects thereof; 用于管理事件响应的文件化

流程，其中包括保存相应问题和行动日志的要求，以涵盖事件发生时间、报告事件的人员、报告对象以及事件的影响；

(iv) The requirement on the Processor to notify the Controller without undue delay if there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Data transmitted, stored or otherwise processed by Processor; and

在出现安全违规行为导致由处理方传输、存储或以其他方式处理的数据被意外或非法破坏、丢失、更改、未经授权的披露或访问的情况下，要求处理方立即通知控制方，不得无辜延误；以及

(v) The Processor security/incident management team should where appropriate work together with the Controller security representatives until the incident or breach has been satisfactorily resolved.
处理方的安全/事件管理团队应酌情与控制方的安全代表合作，直到事件或违规行为得到圆满解决。

(vi) The procedure for reporting, managing and responding to incidents shall be tested at least once a year.
应至少每年对事件的报告、管理和响应程序测试一次。