DATA PROCESSING AGREEMENT
データ処理契約

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.

本データ処理契約（以下「本 DPA」）は、お客様と Dynatrace 間で締結される、Dynatrace 製品およびサービス（有料か無料かを問わない）の利用につき規定した該当する書面による契約、および関連する注文書、付属書と作業明細書（以下、総称して「本契約」）に基づく、お客様のための個人データの処理に適用される条件に関して、当事者間で合意した事項を反映したものです。両当事者が別途データ処理契約を締結していない限り、本 DPA は該当する注文書に記載されている Dynatrace オファリングの開始日から有効になります。

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://assets.dynatrace.com/global/legal/Online-SA-April-2024-Japanese.pdf.

本 DPA は、本契約の条項に従うものであり、本契約に完全に組み込まれ、その一部を構成するものとします。本 DPA は、明示的に記載されている場合を除き、既存のデータ処理契約に取って代わるものとします。個人データに関して、本 DPA と本契約の他の規定との間に矛盾がある場合、本 DPA が支配し、適用されるものとします。本 DPA において使用されているが、定義されていない用語については、https://assets.dynatrace.com/global/legal/Online-SA-April-2024-Japanese.pdf に規定されているのと同じ意味を有します。

1. Definitions. /定義。

(a) "APPI" means the Japanese Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2016).

「APPI」とは、「個人情報の保護に関する法律」（平成 15 年法律第 57 号、平成 28 年改正）をいいます。

(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.

「データ保護法」とは、本契約に基づくお客様の個人データの処理に適用されるすべてのデータ保護およびデータプライバシーに関する法律および規制をいいます。

(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.

「管理者」は、適用されるデータ保護法に基づいて付与されるのと同じ意味を有し、イスラエルのプライバシー保護法に基づく「データベース所有者」および適用される米国の州プライバシー保護法に基づく「事業者」を含みます。

(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. 「お客様の個人データ」とは、Dynatrace 製品およびサービスを使用する過程で、お客様によりまたはお客様に代わって提出、保存、掲示、表示、またはその他の方法で送信された個人データをいい、本契約および/または本 DPA の規定に違反して、お客様によりまたはお客様のために提出、保存、掲示、表示、またはその他の方法で送信された個人データ（制限付き情報等）は除外されます。

(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 グループ」とは、Dynatrace LLC（デラウェア州の有限責任会社）およびその関連会社のうち、本契約および本 DPA の下で Dynatrace 製品およびサービス、ならびに/または関連するサポートやサービスを提供するために Dynatrace を支援することができる 1 社または複数の会社をいいます。

(f) “Europe” means the European Union, European Economic Area (“EEA”), and/or their member states, Switzerland, and the United Kingdom.

「欧州」とは、欧州連合、欧州経済領域（以下「EEA」）、およびその加盟国、スイス、および英国をいいます。

(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」とは、個人データの取扱いと関連する自然人の保護に関する規定および個人データの自由な移動に関する欧州議会および理事会規則 2016/679（一般データ保護規則）をいいます。

(h) “LGPD” means the Lei Geral de Proteção de Dados Pessoais (General Personal Data Protection Act in
Brazil).

「LGPD」とは、Lei Geral de Proteção de Dados Pessoais（ブラジルの一般個人情報保護法）をいいます。

(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.

「個人データの侵害」とは、Dynatrace が送信、保存またはその他の処理をしている間、お客様の個人データの偶発的または違法な破壊、損失、改ざん、不正な開示またはアクセスを引き起こすセキュリティ違反があったことをいいます。

(j) “PIPL” means the China Personal Information Protection Law.

「PIPL」とは、中国個人情報保護法をいいます。

(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.

「個人データ」とは、適用されるデータ保護法に基づき定義される「個人データ」または「個人情報」であって、 Dynatrace がお客様のために収集または受領するものをいいます。個人データには、 Dynatrace がお客様との本契約に基づく各義務の履行とは無関係に取得または処理する情報は含まれません。

(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. 「処理者」は、適用されるデータ保護法に基づいて付与されるのと同じ意味を有し、イスラエルのプライバシー保護法に基づいて定義される「保有者」、および適用される米国の州プライバシー保護法に基づく「サービスプロバイダー」を含みます。

(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.

「標準契約条項」とは、参照することにより本契約に組み込まれる、欧州委員会決定 2021/914/EU により公布された標準契約条項（適宜更新され、修正または置換されたものを含む）をいいます。

(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.

「復処理者」とは、Dynatrace または Dynatrace グループのメンバーが契約して、本契約または本 DPA の条項に基づいて Dynatrace が Dynatrace 製品およびサービスを提供できるようにする処理者をいいます。

(o) “Supervisory Authority” means the government agency, department, or other competent organization with authority over the processing of Personal Data relevant to this DPA.

「監督機関」とは、本 DPA に関連する個人データの処理について権限を有する政府機関、省庁、その他の所轄の組織をいいます。

(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, as updated, amended or replaced from time to time.

「英国補足条項」とは、データ保護法 2018 の第 119A(1)条に基づき英国情報コミッショナー事務局が発行した欧州委員会標準契約条項に対する国際データ移転に関する補足条項（適宜更新、修正または置換されたものを含む）。

(q) “Business”, ″Controller″, “Consumer,” ″Processor,″ “Service Provider,” ″Data Subject″, “Sell,” “Supervisory Authority”, and ″Processing″ (and ″process″) shall have the meanings given under under applicable Data Protection Law.

「事業者」、「管理者」、「消費者」、「処理者」、「サービスプロバイダー」、「データ主体」、「販売」、「監督機関」、および「処理」(および「プロセス」)は、適用されるデータ保護法に基づき付与される意味を有するものとします。

2. Applicability of DPA and Parties' Roles / 本 DPA の適用範囲と両当事者の役割

(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 は、Dynatrace が本契約および本 DPA に基づく義務を履行し、権利を行使するために、お客様の個人データをお客様のために処理することに適用されます。なお、本 DPA は、管理者としての Dynatrace によるお客様の個人データの処理には適用されません。

(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.

お客様は、管理者または処理者で、Dynatrace は処理者です。データ保護法に基づき適用される範囲において、お客様は、Dynatrace をお客様に代わってお客様の個人データを処理する処理者として任命します。

3. Processing of Customer Personal Data / お客様の個人データの処理

(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 製品およびサービスを提供するために Dynatrace が行うお客様の個人データの処理の性質および範囲は、お客様が決定および管理し、別紙 A で補足するものとします。処理の性質、目的および期間、ならびに収集される個人データの種類および Dynatrace が処理する個人データのデータ主体のカテゴリーは、本 DPA の別紙 A に記載されています。お客様は、Dynatrace がお客様データに含まれる実際のデータまたは個人データの種類についていかなる知識も有していないことを認めます。両当事者は、Dynatrace 製品およびサービスに関連する処理の性質および目的に係るお客様の完全かつ最終的な指示が、本契約および本 DPA に記載されていることに同意します。

(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.

指示の変更または修正がある場合は、書面により通知し、両当事者の了解を得るものとします。Dynatrace は、お客様の処理に係る指示が適用されるデータ保護法を侵害する可能性があると合理的に判断した場合、お客様に通知するものとします。このような場合、Dynatrace は、適用されるデータ保護法に違反していると思われるお客様の個人データを処理することを、お客様がその指示を侵害のないように修正するまで拒否する権利を有します。

(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 ttps://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.

お客様が Dynatrace 製品およびサービスを設定することにより Dynatrace がお客様の個人データを取得することになる範囲で、お客様は、適用されるすべてのデータ保護法を常に遵守することを表明し、保証します。お客様と Dynatrace との間において、お客様は、以下につき責任を負うものとします。(i) Dynatrace 製品およびサービスにより取得されるお客様の個人データの範囲をきめ細かく制御するために、 https://docs.dynatrace.com/docs/manage/data-privacy-and-security（データプライバシーの設定を行う方法に関する Dynatrace の説明）に記載されているとおり、Dynatrace データプライバシー設定を行うことで、 Dynatrace を利用する際にお客様の個人データを保護すること、(ii) お客様の個人データの正確性、品質および合法性、ならびにお客様または関連する第三者が個人データを取得した手段。

(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.

お客様が第三者の管理者を代表して行動する処理者である場合、お客様は Dynatrace に対して、Dynatrace を別の処理者として任命することを含め、お客様の個人データに関する指示および行動が、適切な管理者によって承認されていることを保証します。

(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 consents, including from Data Subjects, for the Processing of Customer Personal Data by Dynatrace as contemplated by the Agreement; (iii) Customer's use of the Dynatrace Offerings will not, and will not cause Dynatrace to, violate any Data Protection Laws or other applicable laws or regulations, or any agreement or obligation between Customer and any third party.

お客様は、以下を表明し、保証します。(i) お客様の個人データを処理するための処理者（Dynatraceを含む）の使用について、法律上要求される場合、データ主体に通知すること（必要な場合、Dynatrace 製品およびサービスの利用に関してデータ主体へ通知することを含む）、(ii) Dynatrace によるお客様の個人データの処理について、データ主体からのものを含み、本契約で意図されるとおり、必要なすべての権利、合法的根拠、認可および/または有効な同意を取得しており、かつ、期間中、それらを保有し続けること、(iii) お客様による Dynatrace の提供物の使用は、データ保護法やその他の適用される法律または規制、あるいはお客様と第三者との間の合意や義務に違反せず、また Dynatrace に違反させないものとします。

(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.

お客様は、Dynatrace 製品およびサービスおよび関連するサービスに関して、Dynatrace が本契約に基づく義務を履行するために必要なお客様の個人データのみを Dynatrace に提供するものとします。お客様は、Dynatrace 製品およびサービスの利用が制限付き情報の処理を必要とせず、また処理に適していないこと、および Dynatrace 製品およびサービスの利用を通じて Dynatrace によって処理されることになる制限付き情報は提供しないことを了解します。

4. Requests from Third Parties. / 第三者からの要求。

(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 製品およびサービスにより、お客様は、データ保護法に基づき付与された権利を行使するデータ主体からの要求（以下「データ主体の要求」）、またはお客様の個人データの処理に関連する規制機関もしくは司法機関からの要求についてお客様を支援するために、お客様の個人データにアクセスできます。お客様が Dynatrace 製品およびサービス内の関連するお客様の個人データにアクセスできない場合、またはお客様の個人データへのアクセスがデータ保護法に従って当該要求に応えるのに十分な支援を提供しない場合、また適用されるデータ保護法により要求される場合、Dynatrace は、お客様の要求に応じて、お客様が本契約に基づくお客様の個人データの処理に関連するデータ主体の要求または規制機関

もしくは司法機関からの要求に応じることができるよう、お客様に合理的な支援を提供することに同意します。Dynatrace が管理者としてお客様を特定することができるお客様の個人データに関連して Dynatrace に直接要求がなされた場合、Dynatrace は、不当に遅延することなく、当該連絡をお客様に伝達するものとし、お客様の明示的な承認がない限り、当該要求に応じないものとします。連絡の表面上、当該要求がお客様に関するものであることが合理的に明らかでない場合、または Dynatrace が自ら回答する法的義務を負う場合には、上記により、Dynatrace はデータ主体または規制機関もしくは司法機関と連絡を取ることが禁止されることはありません。

(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.

Dynatrace は、法執行機関またはその他の第三者からの要求により、お客様が管理者である個人データの開示を余儀なくされた場合、お客様が保護命令またはその他の適切な救済措置を求めることができるよう、個人データへのアクセスを提供したり、個人データを提供したりする前に、当該要求についてお客様に通知します。
Dynatrace がお客様に通知することが法的に禁止されている場合、Dynatrace は、あたかも Dynatrace 自身の機密情報がそう要求されているかのように、不当な開示から個人データを保護するための措置を講じます。

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.

援助と協力。処理の性質および Dynatrace が利用できる個人データの性質に従い、適用されるデータ保護法により要求される場合、Dynatrace は、お客様の書面による要求に応じて、お客様の判断により、Dynatrace が実行する処理の種類がデータ保護影響評価、および／または関連するデータ保護当局との事前協議を必要とするときは、お客様に合理的な支援および情報を提供し、また、お客様の個人データの処理に適用される範囲で、データセキュリティおよび個人データ侵害通知に関する適用されるデータ保護法に基づくその他の義務を遵守して、お客様に合理的な支援を提供します。お客様は、本条に基づく義務を履行するために Dynatrace が負担した、無視できない費用を全額 Dynatrace に弁済するものとします。

6. Demonstrable Compliance. Dynatrace agrees to provide information necessary to demonstrate compliance with this DPA upon Customer's reasonable request.

実証可能なコンプライアンス。Dynatrace は、お客様の合理的な要求に応じて、本 DPA の遵守を証明するために必要な情報を提供することに同意します。

7. Audits and Assessments. / 監査と評価。

(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.

適用されるデータ保護法がお客様に監査または評価の権利を付与する場合、当該権利の範囲に従うことを条件として、お客様は、書面で要求することにより、年に1回を限度として、適用されるデータ保護法に従い、お客様の個人データの処理に関連するDynatraceの方針、手順および記録の監査または評価を実施することができます。

(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.

監査を要求する場合、お客様は、監査予定日の少なくとも4週間前までに詳細な監査計画をDynatraceに提出する必要があり、この監査計画には監査範囲、期間、開始日の案を記載するものとします。Dynatraceは、監査計画を確認し、懸念事項や質問があればお客様に連絡します。監査の開始前に、両当事者は、料金、時期、管理の範囲、提供する証拠、および期間を含む詳細な監査計画に合意するものとします。要求された監査範囲が過去12ヶ月以内に同様の監査報告書で扱われ、Dynatraceが監査対象の管理体制に重大な変更がないことを確認した場合、お客様は、その報告書で扱われた管理体制の監査を要求する代わりに、その調査結果を受け入れることに同意します。

(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.

監査や評価は、(i) Dynatraceの通常の営業時間内に行われ、(ii) 両当事者の守秘義務に従わなければなりません。第三者が監査を実施する場合、当該第三者は,Dynatraceの競合他社であってはならず、Dynatraceの事前の同意に従うものとし、監査を実施する前に両当事者と書面による秘密保持契約を締結しなければなりません。

(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.

すべての監査の費用は、お客様の負担となります。Dynatraceに監査に関する支援を提供することを要求する場合、当該監査支援がDynatrace製品およびサービスの提供の際に必要とされるリソースとは異なるリソースの使用を必要とするとき、またはこれに加えて必要とされるときは、当該監査支援は、別個のサービスとみなされます。
Dynatraceは、かかる監査支援を実施する前に、適用される料金を支払う旨のお客様の書面による確認を求めるものとします。

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.

機密保持。Dynatrace は、お客様の個人データを処理することを許可した者（そのスタッフ、代理人、下請業者を含む）が、契約上もしくは法律上の守秘義務またはその他の拘束力のある守秘義務を負うようにするものとします。

9. Security / セキュリティ

(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.

セキュリティ措置。Dynatrace は、最先端の技術、導入コスト、処理の性質、範囲、文脈、目的、および自然人の権利と自由に対する様々な可能性と重大性のリスクを考慮して、お客様の個人データを処理するリスクに見合った水準のセキュリティを保つように考えられた適切な技術的および組織的な措置（以下「セキュリティ措置」）を講じ、維持するものとします。お客様は、Dynatrace による別紙 B で特定されたセキュリティ措置の実施が、本 DPA に基づく義務を遵守する目的で十分であることを確認します。上記にかかわらず、お客様は、Dynatrace 製品およびサービスを安全に利用する責任が独自にあることを認め、同意します。

(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.

個人データの侵害。Dynatrace は、個人データの侵害に気付いた後、適用されるデータ保護法によって Dynatrace に要求される期間内に、不当な遅延なくお客様に通知します。Dynatrace は、個人データの侵害を取り巻く状況の調査を速やかに開始し、その結果をお客様に提供します。Dynatrace は、かかる個人データの侵害の影響を軽減するために、適用されるデータ保護法により要求されるすべての措置を講じるよう努めます。Dynatrace は、お客様の要求に応じて、処理の性質および Dynatrace が入手可能な情報を

考慮した上で、適用されるデータ保護法に基づいてお客様が関連する個人データの侵害を管轄当局および/または影響を受けるデータ主体に通知できるようにするために、お客様の義務の遵守を支援する上で必要な商業上合理的な手段を講じます。個人データの侵害の通知は、電子メールを含む Dynatrace が選択した任意の手段により、お客様の管理者の 1 人または複数人に配信します。お客様の管理者がオンラインポータル上で正確な連絡先情報を維持すること、またお客様の管理者への書面による通知で Dynatrace が要求したとおりにすることは、お客様が単独で責任を負います。本条に基づいて個人データの侵害を報告または対応する Dynatrace の義務をもって、そのような個人データの侵害に関するいかなる過失または責任も Dynatrace が認めたことにはなりません。

10. Sub-processing / 復処理

(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.

お客様は、本 DPA の下で、Dynatrace グループのメンバーを復処理者として任命する一般的な権限を付与し、 Dynatrace および Dynatrace グループのメンバーがさらに復処理者と契約する権限を付与します。Dynatrace 製品およびサービスの復処理者の最新リストについては、https://www.dynatrace.com/company/trustcenter/customers/subprocessors-dynatrace-services/をご覧ください。新しい復処理者または復処理者の変更に関する通知を受けるには、お客様は、https://www.dynatrace.com/company/trustcenter/customers/subprocessors-dynatrace-services/で登録して通知（以下「データ保護通知」）を受け取るようにする必要があります。Dynatrace は、第三者の復処理者の追加または変更を反映するために、変更が発効する 30 日前までに、復処理者リストを更新するものとします。復処理者リストの更新を購読しているお客様には、変更のお知らせが届きます。

(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.

適用されるデータ保護法により要求される範囲において、お客様は、お客様の個人データの保護に関して、新たに任命された復処理者によるお客様の個人データの処理に対して合理的な理由をもって異議を唱える場合、変更の通知が復処理者リストに投稿されてから 15 日以内に、異議を唱える具体的な理由を記載した書面をもって Dynatrace に通知するものとします。顧客からの異議申立ては書面で行い、復処理者のデータ保護に関する懸案の慣行に関する合理的な懸念に基づき、異議の商業的に合理的な理由を示すものとします。異議申し立て後、両当事者は誠意を持って協力し、お客様の合理的な異議に対処し、復処理者の変更を進めるものとします。異議申立から 15 日以内に合意に至らない場合、Dynatrace の選択により、（a）Dynatrace は復処理者にお客様の個人データを処理しないよう指示するか（その場合、Dynatrace 製品およびサービスの機能が停止してお客様が利用できなくなる場合があります）、または（b）お客様は本 DPA および本契約を直ちに解除することができ、Dynatrace はかかる停止日または解除日以降の期間について、前払いされた料金の按分額を速やかに返金します。上記で指定された期間内に Dynatrace が異議を受け取らなかった場合、お客様は新しい復処理者の使用を承認したものとみなされます。

(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 は、（i）各復処理者との間で、当該復処理者が提供するサービスの性質に適する範囲で、データ保護義務（本 DPA に規定されている義務よりも制限が緩やかではない、それと実質的に同等の適切な契約上の義務）を含む書面による契約を締結し、（ii）当該復処理者が本 DPA の義務を遵守すること、および Dynatrace が本 DPA に基づく義務に違反する原因となる当該復処理者の作為または不作為について、引き続き責任を負うものとします。

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.

解除に伴う顧客データの削除。本契約の解除または満了後、お客様の個人データは 30 日以内に削除、またはお客様の選択により返却します。ただし、適用される法律によって保持が義務付けられている場合や、バックアップシステムに保存されている場合はこの限りではありません。その場合は、本 DPA の条件が引き続き適用されるものとします。

12. International Data Transfers / 海外へのデータ転送

(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.

お客様は、Dynatrace およびその復処理者が、EEA、英国、および/またはスイス、イスラエル、および中国から米国を含むがこれらに限定されない、国境線を越えてお客様の個人データを転送することを許可します。EEA またはスイスを発生源とするお客様の個人データが、適用されるデータ保護法に基づく適切なレベルの保護が与えられていないとされる国へ転送される場合（以下「制限付き転送」）、両当事者は、当該転送が、以下のとおり、参照することにより本 DPA に組み込まれる標準契約条項が適用されることに同意します。本 DPA または本契約へ署名することで、標準契約条項およびそれに添付されているすべての付属書に署名したことになります。お客様（以下「データエクスポーター」）から Dynatrace（以下「データインポーター」）へのお客様の個人データの転送が制限付き転送であり、データ保護法により有効な転送メカニズムを導入することが求められる場合、転送は標準契約条項の適用を受けるものとします。

(b) The Standard Contractual Clauses shall be completed as follows:

標準契約条項は、以下のように作成するものとします。

i. Module Two will apply (as applicable); モジュール 2 が適用されます（該当する場合）。

ii. In Clause 7 (Docking), the optional docking clause will apply; 第 7 条（ドッキング）のオプションのドッキング条項が適用されます。

iii. In Clause 8.5 and Clause 16 (d), the certification of deletion will be provided upon data exporter’s written request; 第 8.5 条および第 16 条(d)の削除の証明は、データエクスポーターの書面による要求に応じて行われます。

iv. In Clause 8.9, the audit right shall be carried out in accordance with Section 7 of the DPA; 第 8.9 条の監査権は、本 DPA 第 7 条に従って行使するものとします。

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;

第 9 条（復処理者の使用）において、復処理者に対するオプション 2「一般的な書面による承認」が適用され、事前通知の期間は、本 DPA の第 11 条に規定されるとおりとします。

vi. In Clause 11 (Redress), the optional language shall not apply; 第 11 条（救済）のオプションの文言は適用されないものとします。

vii. In Clause 13 (Supervision), the competent supervisory authority shall be the Commission nationale de l’informatique et des libertes (CNIL). 第 13 条（監督）の管轄監督機関は、情報処理および自由に関する国家委員会（CNIL）であるものとします。

viii. In Clause 14 (f) and Clause 16 (c), the termination right will be limited to the termination of the Clauses; 第 14 条(f)および第 16 条(c)の解除権は、当該条項の解除に限定されます。

ix. In Clause 17 (Governing Law), the Standard Contractual Clauses shall be governed by French law; 第 17 条（準拠法）の標準契約条項の準拠法は、フランス法とします。

x. In Clause 18(b) (Choice of Forum and Jurisdiction), the parties agree that disputes shall be resolved before the courts of France;

第 18 条（b）（裁判地の選択と裁判管轄）において、両当事者は、紛争はフランスの裁判所で解決することに同意します。

xi. Annex 1 of the Standard Contractual Clauses shall be completed with the information set out in Schedule A of this DPA;

標準契約条項の付属書1には、本DPAの別紙Aに記載された情報を記入します。

xii. Annex 2 of the Standard Contractual Clauses shall be completed with the information set out in Schedule B of this DPA; and

標準契約条項の付属書2には、本DPAの別紙Bに記載された情報を記入します。

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.".

標準契約条項に新たに第1条(e)が追加され、以下のようになります。「本条項に適用される範囲において、本条項は、両当事者によるスイス連邦データ保護法の対象となるお客様の個人データの処理にも準用されます。該当する場合、EU加盟国の法律またはEUの監督当局への言及は、スイス連邦データ保護法および本条項の監督当局としてのスイス連邦データ保護・情報コミッショナーが管轄する、お客様の個人データの転送に関するスイスの法律に基づく適切な言及を含むように修正されるものとします。

(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:

Dynatrace が Dynatrace 製品およびサービスを提供する際、英国を発生源とするお客様の個人データをその保護に適切な水準にあるものとして適用される英国法で指定されていない第三国へ転送する場合、標準契約条項は、(i) 第13条に規定されているとおりに使用および作成し、また (ii) 標準契約条項に新たに第1条(f)を追加し、その内容は以下のとおりです。「本契約に適用される限りにおいて、第13条により補足される本条項は、英国データ保護法の対象となる両当事者のお客様の個人データの処理にも準用されます。また、(iii) 英国補足条項は、以下のように作成するものとします。

i. Table 1 of the UK Addendum shall be completed with the information in Schedule A. 英国補足条項の表1には、別表Aの情報を記入します。

ii. Table 2 of the UK Addendum shall be completed with the information located in Section 13 (c) of this DPA. 英国補足条項の表2には、本DPAの第13条(c)に記載された情報を記入します。
iii. Table 3 of the UK Addendum shall be completed as follows: 英国補足条項の表3は、以下のように記入します。

1) The list of parties is set forth in Schedule A;

当事者のリストは、別表Aに記載されています。

2) A description of the transfer is set forth in Schedule A; 転送の詳細は、別表 A に記載されています。

3) A description of the technical and organizational measures is set forth in Schedule B; 技術的および組織的な措置の説明は、別表 B に記載されています。

4) The list of sub-processors is in section 11 of this DPA;
復処理者のリストは、本 DPA の第 11 条に記載されています。

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. 英国補足条項の表 4 を記入するために、インポーターとエクスポーターの双方は、英国補足条項の第 19 条に規定されるとおり、英国補足条項を終了することができる。

(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):

Dynatrace が Dynatrace 製品およびサービスを提供する際、中国を発生源とするお客様の個人データをその保護に適切な水準にあるものとして適用される中国法で指定されていない第三国へ転送する場合、お客様は、（お客様が管理者である場合は）お客様の個人データのエクスポートに関する以下の全ての義務を履行し、または（お客様が処理者である場合は）関連する第三者の管理者が以下の全ての義務を履行したことを確認する責任を負うものとします。

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;

海外でお客様の個人データを受領する者の名称および連絡先、処理の目的および手段、お客様の個人データの区分、ならびにお客様が海外でお客様の個人データを受領する者に対してお客様の個人データに関する権利を行使するための方法および手続を、本人に通知すること。

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;

お客様の個人データをエクスポートするための合法的な根拠を確保し、本人の同意が合法的な根拠である場合は、別途本人の同意を得ること ;

iii. conducting a personal information protection impact assessment on the exporting of Customer Personal Data; and

お客様の個人データのエクスポートに関する個人情報保護影響評価を実施すること。

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.

免除が適用される場合を除き、PIPL および付随する行政規則で求められる適切な保護措置を採用すること

（すなわち、政府のセキュリティ評価に合格すること、署名済みの標準契約条項を提出すること、または認証を取得すること）。

(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.

上記に加え、監督機関が標準契約条項または類似のデータ転送メカニズムを採用、更新または置換した場合、 Dynatrace は、個人データの合法的な転送のために代替コンプライアンス基準を採用し、標準契約条項または英国補足条項を置換または補足したり、他の国につき新しいデータ転送メカニズムを追加したりする権利を留保します。ただし、これらがデータ保護法の下で認められていることを条件とします。Dynatrace は、データ保護通知の登録を行っているお客様に対し、代替コンプライアンス基準の採用について 30 日前に通知します。通知期間終了後、 Dynatrace の通知に記載された通り、自動的に変更が適用されるものとします。

(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.

以下の文書の間に矛盾または不一致がある場合、以下の順序で優先されるものとします。(1) 標準契約条項（ただし、処理者は、本 DPA の第 11 条の規定に従い、その要件を満たすことを条件として復処理者を任命することができる）または国際的なデータ転送に特に適用されるデータ保護法によって要求される同様のメカニズム、(2) 本 DPA、および (3) 本契約。

(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.

Dynatrace がブラジルで適用されるデータ保護法により保護されるお客様のデータを転送する限りにおいて、 Dynatrace は、LGPD に規定されるデータ主体の原則および権利ならびにデータ保護義務を遵守するものとします。

(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.

Dynatrace が日本で適用されるデータ保護法により保護されるお客様のデータを転送する限りにおいて、Dynatrace は、APPI に規定されるデータ主体の原則および権利ならびにデータ保護義務を遵守するものとします。

(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.

Dynatrace が Dynatrace 製品およびサービスを提供する際、イスラエルを発生源とするお客様の個人データをその保護に適切な水準にあるものとして適用されるイスラエル法で指定されていない第三国へ転送する場合、お客様は、お客様の個人データのエクスポートのための合法的な根拠を確保する責任を負うものとします。なお、本 DPA は、2001 年プライバシー保護規則（国際データ転送）により要求される適切な保護措置を採用するための Dynatrace の書面による義務を果たしたことになります。疑義を避けるために、本 DPA の義務は、2001 年プライバシー保護規則（国境外のデータベースへのデータの転送）の第 3 規則に従い、イスラエル国外への情報の転送を促進するためにお客様によって十分であるとみなされます。

13. Supplemental US State Privacy Laws Specific Terms. / 補足的な米国の州プライバシー保護法の特定の条項。

(a) The definition of "Applicable Data Protection Law" includes. "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") and similar consumer privacy laws in other states, in each case, as amended, supplemented or replaced from time to time.

「適用されるデータ保護法」の定義には、米国の州プライバシー法が含まれます。「米国の州プライバシー法」とは、アメリカ合衆国で施行されている個人データの保護および処理に関するすべての州法をいい、カリフォルニア州プライバシー権法（以下「CCPA」）によって改正されたカリフォルニア州消費者プライバシー法、およびその他の州の類似の消費者プライバシー法を含みますが、これらに限定されず、それぞれの場合において随時改正、補足、または置き換えられます。

(b) 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):

Dynatrace が米国の州プライバシー法に従ってお客様の個人データを処理する場合、Dynatrace は、お客様の個人データを処理する際の「サービスプロバイダー」または「処理者」(該当する場合)です。お客様は、本契約に従って Dynatrace 製品およびサービスを提供する限定された特定の目的（「目的」）のために、お客様の個人データを Dynatrace に開示し、またはその他の方法で利用できるようにするものとします。Dynatrace は、以下を行うものとします（また、その復処理者にそう要求するものとします）。

i. comply with obligations applicable to it as a service provider under US State Privacy Laws;

米国の州プライバシー法に基づきサービスプロバイダーまたは処理者として適用される義務を遵守すること。

ii. notify if it can no longer meet its obligations under US State Privacy Laws;

米国の州プライバシー法に基づく義務を果たせなくなった場合は、その旨を通知すること。

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.

以下の目的のためにお客様のコンテンツを「販売」または「共有」(CPPA の定義による)せず、またお客様の個人データを保持、使用または開示しないこと。(1)本目的以外の目的（商業的目的のためにお客様の個人データを保持、使用、開示することを含む）のため、またはその他米国の州プライバシー法により許可された目的のため、または(2)お客様と Dynatrace の直接の取引関係以外の目的のため。また、米国の州プライバシー法により許可されている場合を除き、お客様の個人データを、Dynatrace が他の事業者または個人から受領する個人データまたは他の事業者または個人に代わって受領する個人データ、または Dynatrace が個人とのやり取りから収集する個人データと組み合わせないこと。ただし、かかる組み合わせが、米国の州プライバシー法により許可された事業目的を遂行するために必要な場合を除きます。

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

お客様は、(1)通知により、Dynatrace が米国の州プライバシー法に基づくお客様の義務に合致した方法でお客様の個人データを処理するようにし、また Dynatrace によるお客様の個人データの不正な処理を停止し、是正するために、当事者間で合意された合理的かつ適切な措置を講じる権利を有し、(2)Dynatrace は、お客様の個人データに関する米国の州プライバシー法に基づく義務をもはや果たすことができないと判断した場合、お客様に通知するものとします.

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.

ix. Dynatrace は、お客様に提供される製品およびサービスの対価としてお客様の個人データを受領しないことを認識し、確認するものとします。Dynatrace は、米国の州プライバシー法に基づく義務を理解し、遵守することを証明します。

14. Miscellaneous / 雑則

(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.

本 DPA で修正された場合を除き、本契約は完全に効力を有し続けます。本 DPA の改定は、権限を有する両当事者の代表者が正式に署名した書面により行うものとします。

(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. 本契約または本 DPA に別段の定めがある場合でも、本 DPA、注文または本契約に起因または関連する各当事者およびその関連会社の責任は、契約、不法行為またはその他の責任論に基づくか否かにかかわらず、本契約の「責任の制限」条項に従うものとし、当該条項において当事者の責任とされているものは、本契約および本 DPA（本契約のすべての付属書を含む）に基づき当該当事者およびその関連会社がともに責任を負うことをいいます。Dynatrace は、本 DPA に起因または関連して発生する間接的または派生的な損失、損害、利益の損失、売上の損失、事業の損失、予想される貯蓄の損失、信用の損失または損害（いずれの場合も直接的か間接的かを問わない）につき、お客様に対して責任を負わないものとします。本契約または本 DPA に基づくいずれかの当事者の義務を制限することなく、お客様は、お客様が本 DPA または適用されるデータ保護法に基づく義務を遵守しなかった結果、またはそれに関連して発生したお客様の個人データに関連して Dynatrace が被った責任は、お客様に対する責任であるかのように、本契約（または適用される場合は本 DPA）に基づく Dynatrace の責任限度額に算入され、減額されることに同意するものとします。本 DPA における別段の規定（いずれかの当事者の補償義務を含むが、これらに限定されない）にかかわらず、いずれの当事者も、相手方の GDPR 違反に関連して、GDPR 第 83 条に基づき規制当局または政府機関により相手方に賦課された GDPR の罰金について責任を負いません。

(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 は、本契約の準拠法および管轄権に関する規定に準拠し、これに従って解釈するものとします。ただし、標準契約条項については、本 DPA の第 13 条に定めるところに従うものとします。

SCHEDULE A / 別紙 A

DETAILS OF THE PROCESSING / 処理の詳細

Description of Data Exporter / データエクスポーターの説明

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.

データエクスポーターとは、復処理の場合にはデータエクスポーターとデータインポーターとの間で締結され、この別紙が添付されているデータ処理契約の「お客様」または「Dynatrace」（場合により）とされる組織をいいます

。

Description of Data Importer / データインポーターの説明

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.

データインポーターとは、データエクスポーターとデータインポーターの間で締結され、この別紙が添付されているデータ処理契約の「Dynatrace」または正式に権限を付与された復処理者とされる組織をいいます。

Subject Matter and Duration of the Processing /処理の対象と期間

The subject-matter and duration of the processing is as follows: 処理の対象と期間は、以下の通りです。

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.
両当事者間では、お客様は、Dynatrace 製品およびサービスの利用に関連してお客様が Dynatrace に提供した特定のお客様の個人データの管理者となります。処理の期間は、本契約の期間とします。

Purposes of the Processing / 処理の目的

The processing is necessary for the following purposes: この処理は、以下の目的のために必要となります。

To enable Dynatrace to provide the Dynatrace Offerings to Customer and exercise its rights and obligations under the Agreement.

Dynatrace がお客様に Dynatrace 製品およびサービスを提供し、本契約に基づく権利および義務を行使できるようにするため。

Data Subjects / データ主体

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.

データ主体は以下の通りです。(i) Dynatrace 製品およびサービスの利用をお客様から許可されたユーザー、ならびに (ii) お客様の単独裁量で決定する、お客様の監視対象アプリケーションおよび/またはウェブサイトのユーザーまたは訪問者（お客様の従業員、顧客やクライアント、代理人、請負業者、顧問を含むが、これらに限定されない）。

Type of Personal Data / 個人データの種類

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.

お客様は、Dynatrace 製品およびサービスを利用するために特定の個人データを提供する必要があります。これには、IP アドレスおよび姓名（ユーザーの電子メールアドレスやユーザー認証情報に含まれる場合）などがあります。お客様は、Dynatrace 製品およびサービスに追加の個人データを提供することができますが、その範囲はお客様が単独裁量で決定し管理するものとします。

Special categories of data or sensitive personal data (if appropriate) / 特別なカテゴリーのデータまたは機密性の高い個人データ（該当する場合）

The Personal Data transferred concern the following special categories of data or sensitive personal data: 転送される個人データは、以下の特別な種類のデータまたは機密性の高い個人データに関するものです。

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.

該当しません。お客様は、書面による明示的な同意がない限り、「特別なカテゴリーのデータ」または「機密性の高い個人データ」に分類されるデータを処理するために Dynatrace 製品およびサービスを利用することはできません。

Processing Operations / 処理業務

The personal data transferred will be subject to the following basic processing activities: 転送された個人データは、以下の基本的な処理活動の対象となります。

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 は、Dynatrace 製品およびサービスを提供し、本契約および本データ処理契約の条項に含まれる権利および義務を行使するために必要な場合にのみ、お客様の個人データを処理するものとします。こ

れには、顧客対応、テクニカルサポート、専門サービス、Dynatrace 製品およびサービスの性能および機能の向上、ユーザー認証および通信、アカウント管理が含まれますが、これらに限定されません。

SCHEDULE B / 別紙 B

SECURITY MEASURES / セキュリティ措置

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（本書においては「処理者」ともいいます）は、お客様（本書においては「管理者」ともいいます）のために処理するお客様の個人データに関して、少なくとも以下に記載する技術的および組織的なセキュリティ措置を実施します。このようなセキュリティ措置は、処理者と管理者の間の基礎となる契約（以下「本契約」）の対象となるすべてのお客様の個人データに適用されます。Dynatrace に代わって個人データを処理する可能性のある第三者の復処理者に関連して、当該第三者は個人データを保護するための独自のセキュリティ要件を有します。

Technical measures / 技術的措置

1.1 Authorization / 承認

(a) An authorization system shall be used where different authorization profiles are used for different purposes.

異なる承認プロファイルを異なる目的のために用いる場合は、承認システムを使用しなければなりません。

1.2 Identification / ID

(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.

すべての許可されたユーザーには、上記の目的で固有の個人識別コード（以下「ユーザーID」）を発行する必要があります。ユーザーID は、後からであっても、他者に割り当てることはできません。

(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.

許可されたユーザーの最新の記録を保管し、各人が利用できる認定アクセスを記録し、情報システムへのすべてのアクセスまたはデータ処理の実施のために、識別および認証手順を確立するものとします。ここで用いられている「処理」は、自動化された手段であるか否かにかかわらず、データに対して行われるあらゆる操作または一連の操作を指し、収集、記録、整理、構造化、保存、適応または変更、検索、相談、使用、送信による開示、普及またはその他の方法で利用できるようにすること、整列または結合、制限、消去または破壊などが含まれます。

(c) Passwords shall be modified periodically as set forth in the Information Security Policies. パスワードは、情報セキュリティポリシーに定められたとおり、定期的に変更するものとします。

1.3 Authentication / 認証

(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.

許可されたユーザーは、特定の処理業務または一連の処理業務に関連する認証手順を正常に完了するような認証資格を受けた場合、データを処理することの許可を受けるものとします。

(b) Authentication must be based on a secret password associated with User ID, and which password shall only be known to the Authorized User.

認証は、ユーザーIDに関連付けられた秘密のパスワードに基づいて行われなければならず、そのパスワードは許可されたユーザーのみが知っているものとします。

(c) One or more authentication credentials shall be assigned to, or associated with, an Authorized User.

1 つまたは複数の認証資格は、許可されたユーザーに割り当てられるか、または許可されたユーザーに関連付けら れるものとします。

(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.

パスワードの機密性と完全性を確保するための手順がある必要があります。パスワードは、有効期限内であれば解読できないように保存しなければなりません。パスワードを割り当て、配布し、保管するための手順がある必要があります。

(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.

パスワードは少なくとも 12 文字で構成しなければならず、関連する情報システムで技術的にこれが許可されていない場合は、パスワードは許容されている最大文字数で構成しなければなりません。パスワードには、処理を担当する許可されたユーザーに容易に関連付けることができる項目を含んではならず、定期的に変更しなければなりません。その間隔はセキュリティ文書に定めなければなりません。パスワードは、最初に使用するときおよびその後定期的に、許可されたユーザーが自身のみが知っている秘密の値に変更するものとします。

(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.

有効なユーザーID とパスワードの組み合わせに加え、Dynatrace のデータまたはシステムへのアクセスはすべて、多要素認証（「MFA」）ソリューションによって保護する必要があります。MFA ソリューションは、ソフトウェアによるものでもハードウェアによるものでも構いません。

(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.

許可されたユーザーが解雇された場合、または異動した場合、または情報システムもしくは処理データへのアクセス権限がなくなった場合、認証資格も無効化されるものとします。

1.4 Access controls / アクセス管理

(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.

電子的またはポータブルメディアに保存するとき、または送信するときを含め、データにアクセスできるのは許可されたユーザーに限定するものとします。許可されたユーザーには、職務を遂行するために必要なデータおよびリソースへのアクセスのみを許可するものとします。

(b) A system for granting Authorized Users access to designated data and resources shall be used. 指定されたデータおよびリソースへのアクセスを許可されたユーザーに付与するシステムを使用するものとします。

(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.

半期ごとに、関連する認証プロファイルを保持するための前提条件が依然として適用されていることを検証するものとします。これには、タスクの同種のカテゴリーおよび対応する認証プロファイルを基に作成された許可されたユーザーのリストも含まれる場合があります。

(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.

ユーザーが情報システムに不正にアクセスしたり、使用したりすることを防止するための措置を講じるものとします。特に、不正なアクセスから情報システムを保護するために、業界のベストプラクティスを反映した侵入検知システムを導入する必要があります。

(e) Operating system or database access controls must be correctly configured to ensure authorized access only.

オペレーティングシステムやデータベースのアクセス制御を正しく設定し、許可されたアクセスのみが行われるようにする必要があります。

(f) Only those staff authorized shall be able to grant, alter or cancel access by users to the information systems.

権限を与えられたスタッフのみが、ユーザーによる情報システムへのアクセスを許可、変更、または取り消すことができるものとします。

1.5 Management of computer systems and removable media / コンピュータシステムおよびリムーバブルメディアの管理

(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.

データを保存するネットワーク情報システムおよび物理メディアは、安全な環境に保管し、物理的なアクセスはそのようなアクセスを許可されたスタッフに制限しなければなりません。強力な認証とアクセス管理を維持する必要があります。

(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.

情報システムに使用されているソフトウェア、ファームウェア、ハードウェアは、情報システムの脆弱性や欠陥を検出し、そのような脆弱性や欠陥を解決するために、毎年見直しを行うものとします。

(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.

不正なアクセスや処理を防止するために、データが保存されているメディアの保管と使用に関してポリシーを発行し、トレーニングを実施するものとします。

(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.

メディアを廃棄または再利用する場合は、以前に保存されていたデータおよびその他の情報を後から検索できないようにするか、技術的手段によって情報を理解できないようにするか、再構築できないようにするために必要な措置を講じてから、在庫から取り出さなければなりません。データの保存に使用されるすべての再利用可能なメディアは、ランダム化されたデータで最低 3 回上書きしてから廃棄または再利用するものとします。

(e) The removal of media containing Data from the designated premises must be specifically authorized by the Controller and in compliance with Dynatrace policies.

指定された施設からデータを含むメディアを持ち出すには、管理者の明確な承認を受け、Dynatrace ポリシーに準拠していなければなりません。

(f) Media containing Data must be erased or rendered unreadable if it is no longer used and prior to proper disposal.

データを含むメディアは、使用しなくなった場合、適切に廃棄する前に、消去または読み込めないようにする必要があります。

1.6 Distribution or transmission 配信または送信

(a) Data must only be available to Authorized Users. データを利用できるのは、許可されたユーザーに限定するものとします。

(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.

公共のネットワークを介して電子的に送信されるデータやポータブルデバイスに保存されるデータ、または物理的に安全でない環境でデータを保存または処理する必要がある場合には、暗号化（128 ビット以上）またはその他の同等の保護手段を使用してデータを保護する必要があります。

(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.

メンテナンスのために指定された敷地からデータを持ち出す場合には、データやそこに保存されたその他の情報が不正に取得されないように、必要な措置を講じなければなりません。

(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.

データが電子通信ネットワークを介して送信または転送される場合、データの流れを制御し、送信または転送のタイミング、送信または転送されたデータ、送信または転送されたデータの宛先、および送信または転送を行う許可されたユーザーの詳細を記録するための措置を講じるものとします。

1.7 Preservation, back-up copies and recovery 保存、バックアップコピーと
リカバリー

(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.

バックアップコピーの作成とデータの回復のための手順を定義し、規定しなければなりません。これらの手順は、データが紛失または破壊された時の状態で再構築することにつき規定しなければなりません。

(b) Back-up copies must be made at least once a week, unless no Data have been updated during that period. バックアップコピーは、少なくとも1週間に1度は作成しなければなりません。ただし、その期間中にデータが更新されなかった場合はこの限りではありません。

(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.

データを処理する情報システムのサイトとは別の場所にバックアップコピーとデータ回復手順を保管しなければならず、この最低セキュリティ要件はそのようなバックアップコピーに適用されるものとします。

1.8 Anti-virus and intrusion detection アンチウイルスおよび
侵入検知

(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).

情報システムに対する攻撃やその他の不正行為から保護するために、情報システムにアンチウイルスソフトウェアや侵入検知システムを導入しなければなりません。アンチウイルスソフトウェアおよび侵入検知システムは、当該情報システムの業界のベストプラクティスに従って、定期的に（少なくとも年1回）更新する必要があります。

1.9 Testing / テスト

(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.

情報システムの処理データの実装または変更に先立つテストでは、実際のデータまたは「ライブ」データを使用しないものとしますが、そのような使用が必要であり、合理的な代替手段がない場合はこの限りではありません。実際のデータまたは「ライブ」データを使用する場合は

、テスト目的に必要な範囲に限定し、処理されるデータの種類に対応するセキュリティレベルを保証する必要があります。

1.10 Audit / 監査

(a) Regular audits of compliance with these security requirements, at least annually, should be performed.

このようなセキュリティ要件への準拠について、少なくとも年1回の定期的な監査を実施する必要があります。

(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.

その結果から、採用されたセキュリティ措置および管理がこれらのセキュリティ要件にどの程度まで準拠しているかについての見解を得て、欠点を特定し、（もしあれば）必要に応じて是正措置または補完措置を提案しなければなりません。これには、見解に至った根拠となるデータ、事実および観察、ならびに提案された推奨事項も含める必要があります。

2. Organizational measures / 組織的措置

2.1 Security plan and document / セキュリティ計画とドキュメント

- 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.

これらのセキュリティ要件を遵守するために採用する措置は、当社の情報セキュリティポリシーの対象となり、セキュリティポータルに記載されます。これは常に最新の状態に保ち、情報システムまたは技術的もしくは組織的な措置に関して変更が加えられた場合には常に改訂するものとします。

- The Information Security Policies shall address: 情報セキュリティポリシーでは、以下の事項を取り扱うものとします。

(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;

アプリケーションの開発および保守、適切なベンダーサポート、ハードウェアおよびソフトウェアのインベントリを含む、データ処理に使用されるシステムの変更および保守に関するセキュリティ措置。

(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

物理的セキュリティ（データ処理が行われる建物または敷地のセキュリティ、データ機器および通信インフラのセキュリティ、環境管理を含む）。

(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.

コンピュータおよび電気通信システムのセキュリティ（バックアップコピーの管理手順、コンピュータウイルスに対処する手順、信号/コードの管理手順、ソフトウェア実装のためのセキュリティ、データベースに関するセキュリティ、システムをインターネットに接続するためのセキュリティ、データシステムの回避策の検査、システムのセキュリティの侵害や不正アクセスを試みる行為を記録するためのメカニズムを含む）。

- The security plan shall include all Dynatrace policies, as updated from time to time, including but not limited to:

セキュリティ計画には、以下を含むが、これらに限定されない、随時更新されるすべてのDynatraceポリシーを含めるものとします。

(i) Code of Business Conduct and Ethics 企業倫理・行動規範

(ii)Global Data Protection Policy グローバルデータ保護ポリシー

(iii) Dynatrace IT Acceptable Use Policy
Dynatrace IT利用ポリシー

(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.
システムセキュリティポリシー：Dynatraceアクセス管理ポリシー、バックアップ保持基準、変更管理ポリシー、変更管理ポリシー - ビジネスシステム、コンプライアンスポリシー、サイバーおよびデータセキュリティインシデント対応計画、データ分類ポリシー、データ損失防止ポリシー、電子監視ポリシー、暗号化ポリシー、人事セキュリティポリシー、情報資源管理ポリシー、情報リスク管理ポリシー、ITオペレーションポリシー、モバイルデバイスポリシー、ネットワークアクセスポリシー、ネットワークアカウントパスワードポリシー、ネットワークファイアウォールポリシー、物理的セキュリティと環境ポリシー、解雇された従業員の資産返却ポリシー、セキュア、セキュリティフィッシングポリシー、サービスアカウントライフサイクルポリシー、ベンダー管理ポリシー、脆弱性管理ポリシー、ワークステーションセキュリティポリシー。

(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:
セキュリティ計画は、データおよび情報システムにアクセスするスタッフが利用できるようにし、少なくとも以下の点をカバーしなければなりません。

(vi)The scope, with a detailed specification of protected resources; 範囲（保護されたリソースの詳細な仕様を含む）。

(vii) The measures, standards, procedures, code of conduct rules and norms to guarantee security, including the control, inspection and supervision of the information systems;
セキュリティを保証するための措置、基準、手順、行動規範ルール、標準（情報システムの管理、検査、監督を含む）。

(viii) The procedures for reporting, managing and responding to incidents; and インシデントの報告、管理、対応の手順。

(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.
バックアップコピーの作成およびデータの復元の手順（処理活動を行ったスタッフ、復元されたデータ、および必要に応じて復元プロセスでどのデータを手動で入力しなければならなかったかを含む）。

2.2 Functions and obligations of staff スタッフの職務と義務

- 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”).

  情報システムにアクセスしたり、データの処理を実行したりする正当な業務上の必要性があるスタッフのみに、その実行を許可するものとします（「許可されたユーザー」）。

- 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.

  データ処理に関する職務と義務の遂行、およびこれらの要件に違反した場合の結果について、スタッフを訓練し、これらの最低セキュリティ要件、関連するポリシー、および適用される法律を熟知させるために、必要な手段を採用するものとします。

- The functions and obligations of staff having access to Data and the information systems shall be clearly defined through application security roles.

  データおよび情報システムにアクセスするスタッフの職務および義務は、アプリケーションセキュリティの役割を通じて明確に定義するものとします。

- 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. 許可されたユーザーに、処理セッション中に電子機器を放置したり、アクセスできるようにしたりしてはならないという旨の指示を出すものとします。データが保存されているエリアへの物理的なアクセスは、許可されたユーザーに限定するものとします。セキュリティ計画に違反した場合の懲戒措置は、明確に定義し、文書化し、スタッフに周知するものとします。

2.3 Chief Security Officer / 最高セキュリティ責任者

- 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.

  これらの最低限のセキュリティ要件に全面的に準拠する責任を負う者を、最高情報セキュリティ責任者（以下「CISO」）として任命するものとします。CISO は、情報セキュリティの管理に関して適切な訓練を受け、経験を積み、コンプライアンスを効果的に確保するための適切なリソースの提供を受けるものとします。

- The contact details of the CISO shall be provided to the Controller upon request.

  CISO の連絡先は、要求に応じて管理者に提供するものとします。

2.4 Record keeping / 記録の保存

- A history of Authorized User access to, or disclosure of, Data shall be recorded with a secure audit trail.

  許可されたユーザーによるデータへのアクセスまたはデータの開示の履歴は、安全な監査証跡とともに記録するものとします。

- Only those staff duly authorized may have physical access to the premises where information systems and media storing Data are stored.

  正式に権限を与えられたスタッフのみが、データを保存する情報システムおよびメディアが保管されている施設に物理的にアクセスすることができます。

- There shall be a procedure for reporting, responding to and managing security incidents such as data security breaches. This shall include at a minimum:

  データセキュリティ侵害などのセキュリティインシデントを報告、対応、管理するための手順を用意するものとします。これには少なくとも以下を含めるものとします。

  (i) A procedure for reporting such incidents/breaches to appropriate management; そのようなインシデント/違反を適切な管理職に報告するための手順。

  (ii) A clearly designated team for managing and coordinating the response to an incident led by the CISO; インシデントへの対応を管理および調整するための明確に指定された CISO 率いるチーム。

(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;

インシデントへの対応を管理するための文書化されたプロセス（インシデントが発生した時刻、インシデントを報告した者、報告先、およびその影響を含む適切な問題および行動ログを保管する要件を含む）。

(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

処理者が送信、保存、またはその他の方法で処理したデータの偶発的もしくは違法な破壊、紛失、改ざん、不正な開示、またはアクセスにつながるセキュリティ違反があった場合、処理者は、管理者に遅滞なく通知する必要があります。

(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.

処理者のセキュリティ/インシデント管理チームは、必要に応じて、インシデントまたは違反が十分に解決されるまで、管理者のセキュリティ担当者と協力しなければなりません。

(vi) The procedure for reporting, managing and responding to incidents shall be tested at least once a year. インシデントの報告、管理、対応のための手順は、少なくとも1年に1回テストするものとします。