

DATA PROCESSING AGREEMENT	データの取扱いに関する契約
<p>A. General</p> <p>1. <u>Parties, Service Agreement.</u> This Data Processing Agreement (“DPA”) is between the entity identified below as the Controller (the “Controller”, “Customer” or “Data Exporter”), and Proofpoint, Inc., 925 W. Maude Avenue, Sunnyvale, CA 94085 (“Processor,” “Proofpoint” or “Data Importer”) and is appended to, as applicable: (1) the Proofpoint Master Subscription Agreement or General Terms and Conditions and applicable Product Exhibit(s); (2) an end user license agreement (the online Customer Agreement, a EULA, clickwrap if any, or clickthrough agreement) accepted by Controller on Controller’s initial registration and access of the Proofpoint product or service; or (3) any another written and signed license agreement, including an evaluation agreement, between the parties under which Processor provides products or services to Controller (each, the “Service Agreement”).</p> <p>2. <u>Definitions.</u> Words and expressions used in this DPA but not defined including, without limitation, “business,” “business purpose,” “consumer,” “controller,” “data subject,” “personal data,” “personal information,” “processing,” “processor,” “sell,” “sensitive data,” “service provider,” “sub-processor,” “supervisory authority” and their respective derivative terms, shall have the meanings set forth in the privacy and data protection laws, regulations, and decisions applicable to a party to this DPA (“Applicable Data Protection Law”), which may include, without limitation (i) the EU General Data Protection Regulation (2016/679) (“GDPR”), (ii) the Brazilian General Data Protection Law of 2018, Brazil Federal Law 13.709/2018, Lei Geral de Proteção de Dados, (iii) the Japanese Act on the Protection of Personal Information Act. No.57 of 2003 as amended, and its applicable regulations, and (iv) the California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100 et seq. and its implementing regulations, in each case as amended, superseded or replaced from time to time.</p> <p>3. <u>Processing of Controller Data.</u> The nature and subject matter of the processing carried out by Proofpoint on Controller’s behalf and Controller’s instructions to Proofpoint are described in the Service Agreement (the data so processed shall be hereinafter referred to</p>	<p>A. 総則</p> <p>1. <u>当事者、本サービス契約</u> このデータの取扱いに関する契約（以下「本 DPA」という。）は、以下に管理者として特定される主体（以下「管理者」、「カスタマー」又は「データ提供者」という。）と、カリフォルニア州、94085、サニーベール、ウエスト・モード・アベニュー 925 に事業所を有する Proofpoint, Inc.（以下「受託者」、「Proofpoint」又は「データ受領者」いう。）との間で締結され、（1）プルーフポイント・マスター・サブスクリプション契約（Proofpoint Master Subscription Agreement）若しくは一般取引条件（General Terms and Conditions）及び適用される製品の添付文書、（2）管理者が Proofpoint の製品若しくはサービスに最初に登録及びアクセスした時に承諾したエンドユーザライセンス契約（これには、オンラインの Customer Agreement、EULA 及び該当する場合はクリックラップ又はクリックスルー契約が含まれる。）、又は（3）受託者が製品若しくはサービスを管理者に提供することを定めた、署名された書面によるその他の両当事者間のライセンス契約（評価契約を含む。）（以下それぞれを「本サービス契約」という。）のうち該当するものに別紙として添付される。</p> <p>2. <u>定義</u> 本 DPA で使われているが定義されていない用語及び表現（「事業」、「事業目的」、「消費者」、「管理者」、「本人」、「個人データ」、「個人情報」、「取扱い」、「受託者」、「販売」、「機微データ」、「サービス提供者」、「再委託先」、「監督当局」及びこれら各用語の派生語を含むが、これらに限定されない。）は、本 DPA 当事者に適用されるプライバシー保護及びデータ保護に関する法令及び決定（以下「適用データ保護法令」という。）で定められる意味を有するものとする。適用データ保護法令には、 （i）EU 一般データ保護規則（2016/679）（以下「GDPR」という。）、（ii）2018 年ブラジル一般データ保護法（ブラジル連邦法 13.709/2018）（Lei Geral de Proteção de Dados）、（iii）日本の個人情報の保護に関する法律（平成 15 年法律第 57 号。その後の改正を含む。）及びその適用ある規則、並びに（iv）2018 年カリフォルニア州消費者プライバシー法（カリフォルニア州民法、第 1798.100 条以下）及びその施行規則（いずれも随時改正、代替又は差替えされた場合</p>

<p>as “Controller Data”). The types of personal data and categories of data subjects including, without limitation, the processing operations, are set forth in Schedule 1 to this DPA.</p> <p>4. <u>Rights of Data Subjects</u>. Subject to Applicable Data Protection Law, Processor will, to the extent legally permitted, promptly notify Controller if Processor receives a request from a data subject to exercise the data subject's rights under Applicable Data Protection Law, and reasonably assist Controller in responding to such request. Controller shall review, respond to and otherwise handle any such request at its own responsibility and expense.</p> <p>5. <u>Security Breach</u>. Subject to Applicable Data Protection Law, in the event of a known unauthorized use, disclosure or acquisition by a third party of personal data that compromises the security, confidentiality, or integrity of personal data maintained by Processor (“Security Breach”), Processor will notify Controller in writing of the breach without undue delay and provide periodic updates including any information required by Applicable Data Protection Law. Should Controller deem it appropriate to inform any supervisory authority, data subject or other party, to the extent such notice makes reference to Processor, whether explicitly by name or otherwise, Controller shall inform Processor in advance and consider any changes requested by Processor in good faith.</p> <p>6. <u>Cooperation with Supervisory Authorities</u>. Processor shall provide reasonable assistance to Controller in the cooperation or prior consultation with the supervisory authority in the performance of its obligations under Applicable Data Protection Law. Additionally, in connection with the supervisory authority's request, at Controller's expense Processor shall make reasonable efforts to acquire the reasonable cooperation and assistance of sub-processors in providing access to relevant information needed to fulfil Controller's obligations under Applicable Data Protection Law.</p> <p>7. <u>Confidentiality of Controller Data</u>. Processor will not disclose to any third-party government body or public authority, any Controller Data, except in each case, as necessary to comply with applicable law or regulation, or a valid and binding order of a governmental body (such as a subpoena or</p>	<p>は当該変更後の法令を含む。)を含むが、これらに限定されない。</p> <p>3. <u>管理者データの取扱い</u> Proofpoint が管理者に代わって行う取扱い及び管理者の Proofpoint に対する指示の性質及び主題は、本サービス契約に記載されるとおりとする（そのように取り扱われるデータを本 DPA において「管理者データ」という。）。個人データの種別及び本人の分類（取扱いの態様を含むが、これに限定されない。）は、本 DPA の別紙 1 に記載されるとおりとする。</p> <p>4. <u>本人の権利</u> 適用データ保護法令に従うことを条件に、受託者は、適用データ保護法令に基づく本人の権利を行使する旨の要求を本人から受け取った場合、法的に許容される限度において、速やかに管理者に通知し、かかる要求に対応するにあたり管理者を合理的に支援する。管理者は、自らの責任と費用負担でかかる要求を審査し、それに対応し、その他の対処を行う。</p> <p>5. <u>セキュリティ違反</u> 適用データ保護法令に従うことを条件に、受託者は、受託者が保持する個人データのセキュリティ、機密性又は完全性を損なうような、第三者による個人データの不正な使用、開示又は取得（以下「セキュリティ違反」という。）を把握した場合、かかるセキュリティ違反について遅滞なく管理者に書面で通知し、適用データ保護法令により要求される情報を含む定期的なアップデートを提供する。監督当局、本人又はその他の当事者に通知することが適切であると管理者が判断する場合、当該通知が（明示的に名前を挙げるものか、その他の方法によるかを問わず）受託者に言及する範囲で、管理者はその旨を受託者に事前に通知し、受託者から要求される変更について誠実に検討するものとする。</p> <p>6. <u>監督当局への協力</u> 受託者は、管理者が適用データ保護法令に基づく義務の履行にあたって監督当局との協力又は事前協議を行う際に、管理者に対し合理的な支援を提供するものとする。また、監督当局の要請に関連して、受託者は、適用データ保護法令に基づく管理者の義務の履行に必要な関連情報へのアクセスを提供するために、管理者の費用負担で、再委託先から合理的な協力及び支援を得るよう合理的な努力を行うものとする。</p> <p>7. <u>管理者データの機密性</u> 受託者は、適用ある法令又は政府機関の有効かつ拘束力ある命令（例えば、召喚状、裁判所命令など）に従うために必要な場合を除き、第三者であ</p>
---	--

<p>court order). If a governmental body sends Processor a demand for sensitive Controller Data, Processor will attempt to redirect the governmental body to request this data directly from Controller. As part of this effort, Processor may provide Controller's basic contact information to the governmental body. If compelled to disclose Controller Data to a governmental body, then Processor will give Controller reasonable notice of the demand to allow Controller to seek a protective order or other appropriate remedy unless Processor is legally prohibited from doing so. Under the United States' Foreign Intelligence Surveillance Act (FISA), Processor is a "remote computing service" and not a telecom provider and therefore unlikely (in Processor's opinion) to be the subject of a government request under such laws.</p> <p>8. <u>Security of Personal Data.</u> Processor shall at a minimum implement the technical and organizational measures specified in Schedule 1 to ensure the security of personal data. Processor shall grant access to personal data undergoing processing to members of its personnel only to the extent necessary for implementing, managing and monitoring the Service Agreement. Processor shall ensure that persons authorized to process personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.</p> <p>9. <u>Appointment of Subprocessors.</u> Controller hereby provides general consent to Processor to use Subprocessors. Controller acknowledges and agrees that (a) Processor's affiliates may be retained as Subprocessors, and (b) Processor and its affiliates respectively may engage third-party Subprocessors in connection with the provision of the Services. Processor or its affiliate(s) engaging a Subprocessor shall enter into a written agreement with each such Subprocessor containing data protection obligations not less protective than those in this DPA with respect to the protection of Controller Data to the extent applicable depending on the nature of the service provided by such Subprocessor. Processor shall remain fully responsible to Controller for the performance of Subprocessors' obligations in accordance with its contract with Processor or its affiliate(s).</p> <p>10. <u>Verification and Audit.</u> Processor shall make</p>	<p>る政府機関又は公的当局に対して管理者データを開示しない。政府機関が受託者に対し機微にわたる管理者データの開示を要求する場合、受託者は、当該政府機関にデータの開示を管理者に直接要求させるように試みるものとする。かかる試みを行う際、受託者は、管理者の基本的な連絡先情報を当該政府機関に提供することができる。政府機関に対する管理者データの開示を余儀なくされた場合、受託者は、法的に禁じられない限り、管理者が保護命令その他の適切な救済を求めることができるよう、管理者に対し開示要求に関する合理的な通知を行う。米国の外国情報監視法（FISA）の下で、受託者は「リモートコンピューティングサービス」に該当し、テレコムプロバイダーには該当しないため、（受託者の見解では）受託者が同法に基づく政府の要求を受ける可能性は低い。</p> <p>8. <u>個人データのセキュリティ</u> 受託者は、個人データのセキュリティを確保するため、少なくとも、別紙 1 に記載する技術的及び組織的措置を講ずるものとする。受託者は、本サービス契約の履行、管理及び監視に必要な範囲に限り、自社の人員に取扱い中の個人データへのアクセスを付与するものとする。受託者は、受領した個人データを取り扱う権限を有する者が秘密保持を確約し、又は法令に基づく適切な秘密保持義務を負うことを確保するものとする。</p> <p>9. <u>再委託先の選任</u> 管理者は、受託者が再委託先を使用することに一般的に同意する。管理者は、(a) 受託者の関係会社が再委託先ととなることができること、並びに (b) 受託者及びその関係会社はそれぞれ、本サービスの提供に関して、第三者たる再委託先を選任できることを確認し、これに同意する。再委託先を選任する受託者又はその関係会社は、各再委託先と、当該再委託先が提供するサービスの性質に応じて適用される範囲で、管理者データの保護に関して本 DPA が課すデータ保護義務と同等以上のデータ保護義務が含まれる契約を締結するものとする。受託者は、再委託先が、受託者又はその関係会社との契約に従ってその義務を履行することについて、管理者に対し全ての責任を負うものとする。</p> <p>10. <u>検証及び監査</u> 受託者は、書面による合理的な要請があった場合、別途そのための秘密保持契約を締結することを条件として、受託者が本 DPA に基づく義務を遵守していることを証明するために必要な管理者の個人データの取扱いに関する情報を管理者に</p>
---	--

<p>available to Controller, upon reasonable written request and subject to the execution of a dedicated non-disclosure agreement, information related to the processing of personal data of Controller as necessary to demonstrate Processor's compliance with the obligations under this DPA. Processor shall allow for onsite inspection requests by Controller or an independent auditor in relation to the processing of personal data to verify that Processor is in compliances with this DPA, if (a) Processor has not provided sufficient written evidence of its compliance with the technical and organizational measures; (b) a Security Breach has occurred; (c) an inspection is officially required by Controller's supervisory authority; or (d) Applicable Data Protection Law provides Controller with a mandatory on-site inspection right; and provided that Controller shall not exercise this right more than once per year unless Applicable Data Protection Law requires more frequent inspections. Such facility inspections shall be conducted in a manner that does not impact the ongoing safety, security, confidentiality, integrity, availability, continuity and resilience of the inspected facilities, and/or otherwise expose or compromise any confidential data processed therein. Each party shall bear its own cost associated with any audit or inspection. This shall also apply to any provision of information or audit pursuant to Section 8.9 (c-e) of the Standard Contractual Clauses.</p> <p>11. <u>Termination</u>. Controller acknowledges and agrees that in the event of a suspension or termination of any data processing under this DPA or Clause 18 of the Standard Contractual Clauses, the timeframe for Processor's cessation of all processing and deletion of personal data will be governed by the retention periods set forth at www.proofpoint.com/legal/trust/product_processing_operations.</p>	<p>提供するものとする。受託者は、(a) 受託者がその技術的及び組織的措置の遵守に関する十分な書面による証拠を提供していない場合、(b) セキュリティ違反が発生した場合、(c) 管理者の監督当局が正式に検査を要請した場合、又は (d) 適用データ保護法令に基づき、管理者に強制立入検査を行う権利が付与される場合には、管理者又は独立監査人が、受託者が本 DPA を遵守していることを確認するために、個人データの取扱いに関して立入検査を行うことを認める。ただし、適用データ保護法令がより高い頻度で検査を行うことを義務づけていない限り、管理者はかかる権利を年に一度を超えて行使しないものとする。当該立入検査は、検査対象施設の継続的な安全性、セキュリティ、機密性、完全性、可用性、継続性及び障害耐性に影響せず、かつ／又はその他の態様で当該施設内で取り扱われる機密データを公開若しくは漏洩されない態様で行うものとする。各当事者は、監査又は検査に関連する自己の費用を負担するものとする。この規定は、標準契約条項第 8.9 条 (c-e) に基づく情報提供及び監査にも適用されるものとする。</p> <p>11. <u>終了</u> 管理者は、本 DPA 又は標準契約条項第 18 条に基づくデータの取扱いが停止又は終了した場合、受託者による全ての取扱いの終了及び個人データの削除は www.proofpoint.com/legal/trust/product_processing_operations に定める保管期間に準拠することを確認し、これに同意する。</p>
<p>B. Processing and Transfer of Data in the EU</p> <p>The parties agree that with respect to EU Personal Data, all data processing shall be in compliance with the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR"). Proofpoint is certified under the EU-U.S. Data Privacy Framework ("DPF"), adheres to DPF principles, and has extended its DPF certification to include</p>	<p>B. EU におけるデータの取扱い及び移転</p> <p>両当事者は、EU 域内の個人データについて、全てのデータの取扱いが 2016 年 4 月 27 日付け欧州議会及び欧州理事会の EU 一般データ保護規則 (2016/679) (以下「GDPR」という。)を遵守しなければならないことに同意する。Proofpoint は、EU・米国データプライバシーフレームワーク (以下「DPF」という。)に基づ</p>

the UK-US Data Bridge. Such certification and extension can be found at <https://www.dataprivacyframework.gov>.

Solely for the provision of Service under the Service Agreement, personal data may be transferred to and stored and/or processed in any country in which Processor or its sub-processors operate, which may include third party countries. All transfers of personal data out of the European Economic Area shall be governed by the Standard Contractual Clauses annexed to the EU European Commission Decision (EU) 2021/914 (the “**SCCs**”) Module 2 (Controller to Processor). Proofpoint provides the option to its customers to choose one, or both, of these data transfer mechanisms as the legal basis to transfer personal data from the EU to the US, and to process such personal data in the US. If Controller opts to use the SCCs, the parties agree to incorporate such SCCs by reference as follows:

1. *Optional clauses*: none of them are included and applicable between the parties, except as set forth below.
2. *Clause 7, Docking Clause* shall apply for any of Controller’s Affiliates entitled to access the Services pursuant to the Service Agreement.
3. *Clause 9 option 2*: general authorisation for sub-processors and the parties agree that the time period for notification of changes to sub-processors shall be 30 days.
4. *Clause 13 (Supervision)*: shall be as follows:
 - a. Where Controller or a Controller affiliate is established in an EU member state, the supervisory authority with responsibility for ensuring compliance by Controller or a Controller affiliate with the Applicable Data Protection Law as regards the data transfer shall act as competent supervisory authority.
 - b. Where Controller or a Controller affiliate is not established in an EU member state the Netherlands supervisory authority shall act as competent supervisory authority.
5. *Clause 17 (Governing law)*: the clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The parties agree that this shall be: (a) the laws of the

く認証を受け、DPF の原則に従っており、これに英米データブリッジを含めるよう DPF の認証を拡張している。この認証及び拡張については、<https://www.dataprivacyframework.gov> を参照のこと。

個人データは、本サービス契約に基づく本サービス提供の目的のためにのみ、受託者又はその再委託先が業務を行う国（第三国を含む。）に移転し、かかる国で保存及び／又は取扱いをすることができる。欧州経済地域からの個人データの移転は全て、欧州委員会決定 (EU) 2021/914 に付属する標準契約条項（以下「**SCC**」という。）モジュール 2（管理者から受託者への移転）に準拠するものとする。Proofpoint はその顧客に対し、個人データを EU から米国に移転する法的根拠としてこれらデータ移転の仕組みのうちいずれか又は両方を選択し、かかる個人データを米国で取り扱うオプションを提供する。管理者が SCC の利用を選択した場合、両当事者は以下のとおりに SCC を参照により本 DPA に組み込むことに同意する。

1. *選択条項*: 以下に定めるものを除き、いずれも含まれず、両当事者間に適用されない。
2. *第 7 条、ドッキング条項*は、本サービス契約に基づき本サービスにアクセスする権利を有する管理者の関係会社に適用される。
3. *第 9 条オプション 2*: 再委託先の一般的な承認。両当事者は、再委託先への変更通知期間を 30 日とすることに合意する。
4. *第 13 条（監督）*: 以下のとおりとする。
 - a. 管理者又は管理者の関係会社が EU 加盟国で設立された場合、データ移転に関して管理者又は管理者の関係会社による適用データ保護法令の遵守を確保する責任を負う監督当局が、管轄監督当局となるものとする。
 - b. 管理者又は管理者の関係会社が EU 加盟国以外で設立された場合、オランダの監督当局が管轄監督当局となるものとする。
5. *第 17 条（準拠法）*: 規定はいずれかの EU 加盟国の法に準拠する。ただし、当該法により第三者受益権が認められる場合に限る。両当事者は、これが (a) 本サービス契約がいずれかの EU 加盟国の法に準拠する場合は本サービス契約に定める EU 加盟国の法、(b) 本サービス契約が第三国の法律に準拠する場合はオランダの法

<p>country specified in the Service Agreement if the Service Agreement is governed by the laws of an EU member state, or (b) the laws of the Netherlands if the Service Agreement is governed by the laws of a third country.</p> <p>6. <i>Clause 18 (Choice of forum and jurisdiction)</i>: the parties agree that those shall be the courts (i) specified in the Service Agreement if the Service Agreement has appointed a court of an EU member state, or (ii) the courts of Amsterdam if the Service Agreement has appointed a court of a third country.</p>	<p>であることに同意する。</p> <p>6. 第 18 条（裁判所及び管轄の選択）：両当事者は、(i) 本サービス契約がいずれかの EU 加盟国の裁判所を指定する場合は本サービス契約に指定された裁判所、(ii) 本サービス契約が第三国の裁判所を指定している場合はアムステルダム裁判所とすることに同意する。</p>
<p>C. Transfers from other countries:</p> <p>If the parties have ticked any of the following sections, the respective additional terms shall apply for the processing of data for data subjects in those countries:</p> <p><u>Switzerland</u></p> <p>In respect of Swiss personal data, the SCCs and the selections set out above in Section B for EU Personal Data shall apply, except that:</p> <ol style="list-style-type: none"> 1. The competent supervisory authority under the clause 13 of the EU SCCs shall be the Swiss Federal Data Protection and Information Commissioner. 2. The applicable law for contractual claims under clause 17 of the EU SCCs shall be Swiss law and the place of jurisdiction for actions between the parties pursuant to clause 18 (b) shall be the Swiss courts. 3. Reference to the GDPR in the SCCs are to be understood as references to the Swiss Federal Data Protection Act of 19 June 1992 or any successor thereof. 4. The term “member state” in the EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with clause 18 (c) of the EU SCCs. <p><u>United Kingdom</u></p> <p>In respect of UK Personal Data, the UK Addendum shall apply but, as permitted by clause 17 of such addendum, the Parties agree to change the format of the information set out in</p>	<p>C. その他の国からのデータ移転</p> <p>両当事者が以下の項のいずれかを選択した場合、各追加規定が当該国の本人のデータの取扱いに適用されるものとする。</p> <p><u>スイス</u></p> <p>スイス国内の個人データに関しては、SCC 及び EU 域内の個人データについて上記セクション B に記載された選択が適用される。ただし、以下を例外とする。</p> <ol style="list-style-type: none"> 1. EU SCC 第 13 条に基づく管轄監督当局は、スイス連邦データ保護情報コミッショナーとする。 2. EU SCC 第 17 条に基づく契約上の請求に関する適用法はスイス法とし、第 18 条 (b) に基づく両当事者間の訴訟の管轄地はスイスの裁判所とする。 3. SCC における GDPR への言及は、1992 年 6 月 19 日のスイス連邦データ保護法及びその後継法への言及とみなされるものとする。 4. EU SCC における「加盟国」という用語は、スイス国内の本人が EU SCC 第 18 条 (c) に基づきその常居所（スイス）における自らの権利を行使する可能性を排除するような方法で解釈してはならない。 <p><u>英国</u></p> <p>英国内の個人データに関して、英国補遺が適用されるが、当該補遺第 17 条で認められるように、両当事者は補遺の第 1 部に記載される情報フォーマットを以下のとおりに変更することに同意する。</p> <ol style="list-style-type: none"> 1. 表 1 の両当事者の詳細は、別添 1（署名は不要とする。）に記載のとおりとする。 2. 表 2 の目的において、補遺は EU SCC

Part 1 of the addendum so that:

1. the details of the parties in table 1 shall be as set out in Annex I (with no requirement for signature);
2. for the purposes of table 2, the addendum shall be appended to the EU SCCs (including the selection of modules and disapplication of optional clauses as noted in Section B above; and
3. the appendix information listed in table 3 is set out in Annex I, II and III.
4. For table 4, neither party may end the UK Addendum as per Section 19.
5. The UK Information Commissioner's Office shall act as competent supervisory authority.

Other Countries

In jurisdictions where the DPF and/or the GDPR do not apply, the parties will conform to the principles of the DPF and the terms of this DPA.

IN WITNESS WHEREOF, Proofpoint and Customer represent and warrant to the other that the person entering into this DPA is authorized to sign this DPA on behalf of their respective party.

Customer:

Signature:

Individual Signing:

Title:

Signing Date:

Proofpoint, Inc.:

Signature:

Individual Signing:

Kyle Chin

(上記セクション B に記載のモジュールの選択及びオプション条項の不適用を含む。)に添付されるものとする。

3. 表 3 に記載の追加情報は、別添 I、II 及び III に記す。

4. 表 4 については、いずれの当事者も第 19 条に従い英国補遺を終了させることはできない。

5. 英国情報コミッショナーオフィスが管轄監督当局となるものとする。

その他の国

DPF 及び／又は GDPR が適用されない法域においては、両当事者は DPF の原則及び本 DPA の規定に従う。

以上を証して、Proofpoint 及びカスタマーは、他方当事者に対し、本 DPA を締結する者が各当事者を代表して本 DPA に署名する権限を有することを表明し保証する。

カスタマー :

署名 :

署名者 :

役職 :

署名日 :

Proofpoint, Inc. :

署名 :



署名者 :

Kyle Chin

役職 :

GVP, General Counsel

署名日
11/18/2025

<div>Title:</div> <div>GVP, General Counsel</div> <div>Signing Date:</div>	
<div>SCHEDULE 1</div> <div>ANNEX I</div> <div>A. LIST OF PARTIES</div> <div> <p>Data exporter(s): The data exporter is the identified as Controller on page 1 of this DPA.</p> <p>Data importer(s): The data importer is Proofpoint, Inc., a provider of email and social media security services, threat analytics, security training, and other security services.</p> </div> <div>B. DESCRIPTION OF TRANSFER</div> <div> <p>Data subjects are Controller's employees and contractors, and the employees and contractors of Controller's customers and vendors.</p> <p>Categories of data: The categories of data are identified in the table located at www.proofpoint.com/legal/trust/product-processing-operations.</p> <p>Processing operations: The frequency of transfer, nature and purpose of the processing, retention period are identified in the table located at https://www.proofpoint.com/us/legal/trust/product-processing-operations.</p> </div> <div>C. COMPETENT SUPERVISORY AUTHORITY</div> <div> <p><i>Identify the competent supervisory authority/ies in accordance with Clause 13</i></p> <p>As set forth in Section B.4.a of this DPA.</p> <p>_____</p> </div>	<div>別紙 1</div> <div>別添 I</div> <div>A. 当事者一覧</div> <div> <p>データ提供者：データ提供者は本 DPA の 1 頁に管理者として特定される。</p> <p>データ受領者：データ受領者は、メール及びソーシャルメディアセキュリティサービス、脅威分析、セキュリティトレーニングその他のセキュリティサービスの提供事業者である Proofpoint, Inc.である。</p> </div> <div>B. データ移転の詳細</div> <div> <p>本人は、管理者の従業員及び業務受託者、並びに管理者の顧客及びベンダーの従業員及び業務受託者である。</p> <p>データの分類：データの分類については、 www.proofpoint.com/legal/trust/product-processing-operations の表を参照のこと。</p> <p>取扱いの態様：移転の頻度、取扱いの性質及び目的、並びに保管期間については、 https://www.proofpoint.com/us/legal/trust/product-processing-operations の表を参照のこと。</p> </div> <div>C. 管轄監督当局 第 13 条に従って管轄監督当局を特定すること。</div> <div> <p>本 DPA のセクション B.4.を参照のこと。</p> <p>_____</p> </div>

<p>ANNEX II</p> <p>TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA</p> <p>The current Technical and Organizational Measures can be found at www.proofpoint.com/legal/trust/technical-and-organizational-measures</p> <p>ANNEX III</p> <p>The current list of sub-processors for the Service is available on the Proofpoint Trust Site at: https://www.proofpoint.com/us/legal/trust/subprocessors. In the event Processor makes any changes or additions to such list, to the extent Controller has subscribed to receive notifications on the Trust Site, Processor shall provide notice of such changes by e-mail. The parties agree that this notification satisfies the notification requirements of Section 28.2 of the GDPR and Clause 9 of the SCCs.</p>	<p>別添 II</p> <p>技術的及び組織的措置（データのセキュリティを確保するための技術的及び組織的措置を含む。）</p> <p>現行の技術的及び組織的措置については、www.proofpoint.com/legal/trust/technical-and-organizational-measuresを参照のこと。</p> <p>別添 III</p> <p>本サービスの再委託先の最新の一覧は、Proofpoint Trust Site（https://www.proofpoint.com/us/legal/trust/subprocessors）を参照のこと。受託者は、この一覧の変更又は追加を行う場合、管理者が Trust Site で通知を受け取ることに同意している範囲で、当該変更を電子メールで通知する。両当事者は、この通知が GDPR 第 28 条第 2 項及び SCC 第 9 条の通知要件を満たすことに同意する。</p>
---	---