Data Processing Appendix
（データ処理に関する別紙）

この「データ処理に関する別紙」（以下「本DPA」といいます。）は、「HENNGE One サービス規約」（以下「サービス規約」といいます。）の一部をなすものであり、サービス規約に基づきHENNGE（以下「処理者」）といいます。）がお客様（以下「管理者」といいます。）に提供するHENNGE Oneサービス（以下「本サービス」といいます。）の一環として、処理者が管理者の代わりに行う個人データの処理を規律するものです。本DPAにおいて別途定義のある場合を除き、本DPAにおいて使用する用語には、サービス規約の定義が適用されます。本DPAとサービス規約の条項の間に矛盾が生じた場合、本DPAの条項が優先するものとします。

第１条 定義

1. 「適用されるデータ保護法」とは、本DPAに基づく個人データの処理に適用されるプライバシー権を保護する法令をいい、欧州議会および理事会が2016年4月27日に採択した一般データ保護規則（EU規則2016/679）（以下「GDPR」といいます。）、2018年データ保護法（「DPA 2018」）、英国一般データ保護規則（DPA 2018の第3条(10)（第205条(4)により補充されたもの）に定義される意味を有するもの）（以下「UK GDPR」といいます。）、個人情報保護法（平成15年5月30日法律第57号）（以下「APPI」といいます。）を含みますが、これらに限定されるものではありません。
2. 「データ主体」とは、識別可能な自然人を指し、特に、識別番号、位置データ、オンライン識別子、または当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的もしくは社会的な同一性を示す一つまたは複数の要素を参照することによって、直接的または間接的に、識別されうる者をいいます（他の情報への容易な参照を可能にし、これにより特定の個人を識別できる情報を含みます）。または、適用されるデータ保護法において別途定義される内容を含みます。
3. 「個人データ」とは、特定のデータ主体に関する個人を特定可能な情報を指し、または適用されるデータ保護法において別途定義される内容を含みます。
4. 「個人データの漏洩」とは、偶発的または違法な、破壊、喪失、改変、無権限に開示されまたは無権限にアクセスを導くような、送信され、記録保存され、またはその他の取扱いが行われる個人データの安全性に対する侵害を意味します。または、適用されるデータ保護法において別途定義される内容を含みます。
5. 「処理（個人データの処理）」とは、自動的な手段によるか否かを問わず、収集、記録、編集、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、又は、それら以外に利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊のような、本サービスの一環として処理者が個人データに対して行う業務遂行又は一群の業務遂行をいいます。または、適用されるデータ保護法において別途定義される内容を含みます。

第２条 各当事者の役割及び処理の内容

本DPAに基づく個人データの処理の内容は、以下のとおりとし、別紙１に記載します。

処理の性質及び目的（nature and purposes of the processing）	Ａ行に記載する。
処理の対象（subject matter of the processing）	Ｂ行に記載する。
データ主体の類型（categories of data subjects）	Ｃ行に記載する。
個人データの種類（type of personal data）	Ｄ行に記載する。
処理の期間（duration of the processing）	E行に記載する。

第３条 管理者の義務及び権利

１．管理者は、個人データの処理の適法性の評価及びデータ主体の権利の保護措置について責任を負います。

２．本DPA上の義務及び責任を履行するにあたって、一方の当事者が費用、経費及び損害等（データ主体を含む第三者から本DPAに関する請求を受けたことに起因するもの及び一方の当事者の指示に基づく個人データの処理に起因するものを含みます。）を負担した場合、その発生の原因が他方当事者の責めに帰すべき事由によるものである場合には、当該一方の当事者は他方当事者に対して、かかる費用、経費及び損害等の支払いを請求することができます。本DPAに関連して行われた監督機関による措置に起因して、一方の当事者に生じた費用、経費及び損害等についても同様とします。

第４条 処理者の義務及び権利

１．処理者は、以下の各号の義務を負います。

（１） 個人データの第三国又は国際機関に対する移転（以下「越境データ移転」といいます。）に関連する場合を含め、サービス規約および本DPA（いずれも随時修正された場合には修正後のものを指します。）に規定された、管理者の文書化された指示に基づいてのみ個人データを処理すること。但し、処理者に適用される法令により処理が義務付けられる場合を除きます。本但書きの場合、処理者は、当該法令が公共の利益上の重要な法的根拠に基づく情報提供を禁止していない限り、管理者に対し、処理の前に当該法令上義務付けられる内容について通知するものとします。

（２） 個人データの処理を承認された処理者の従業員が、自ら守秘義務を課し、又は適切な法律上の守秘義務の下にあることを確保すること。処理者は、本DPAに基づく個人データの処理のために実際に必要な範囲内でのみ、その従業員が個人データを利用できるようにするものとします。

（３） 処理者は、本DPA第７条に従い、別紙2に定める「特定の組織的および技術的セキュリティ措置」を講じること

（４） 別の処理者を業務に従事させる場合、本DPA第５条に定める条件を遵守すること

（５） 適用されるデータ保護法に定めるデータ主体の権利行使の請求に対処する義務を管理者が履行するにあたって、本DPAの対象となる個人データの処理の性質を考慮に入れた上で可能な範囲内で、適切な技術的・組織的措置によって管理者を支援（受領した権利行使の請求を速やかに管理者に転送することを含むが、これらに限られない）すること。

（６） 本DPAの対象となる個人データの処理の性質及び処理者が利用可能な情報を考慮に入れた上で、管理者による適用されるデータ保護法に定める義務の遵守の確保を支援すること。特に、処理者において本DPAの対象となる個人データについて個人データ侵害があったことを認識した場合には、当該個人データの処理の性質及び処理者が利用可能な情報を考慮に入れた上で、過度に遅滞することなく、管理者に対し当該個人データ侵害を通知し、当該個人データ侵害に関して管理者が適用されるデータ保護法に基づく通知及び連絡を行うことを支援しなければなりません。

（７）　本サービスの提供が終了した後、本DPAの対象となる全ての個人データ（複製物を含む）を消去すること。但し、適用されるデータ保護法により個人データの保存が義務付けられる場合を除きます。処理者は、データが消去されるまでの間、引き続き本DPAの遵守を確保するものとします。
（８）　データ保護責任者を任命すること。
（９）　役職員（契約形態を問わず処理者または処理者の関連会社の業務に従事する者をいい、派遣社員及び業務委託先を含みます。）に個人データを取扱わせるにあたっては、当該個人データの安全管理が図られるよう、当該役職員に対する必要かつ適切な監督をおこなうこと。
（１０）適用されるデータ保護法に基づき許可された場合にのみ個人データを第三者に提供または開示すること。
（１１）適用されるデータ保護法において処理者が義務付られている場合には、本条の定める義務の遵守を証明するために必要な全ての情報を管理者が利用できるようにすること、及び、管理者によって行われる合理的な検査若しくは管管理者から委任された別の監査人によって行われる合理的な検査を含め、監査を受け入れ、若しくは、監査に資するようにすること。当該監査の開始前に、本当事者らは監査の範囲、時期及び期間並びに監査に要する処理者の費用の管理者による負担について相互に合意するものとします。

２．処理者は、その見解において、管理者から出された指示が適用されるデータ保護法に違反すると思料する場合、直ちに管理者に通知するものとします。

第５条 復処理者による処理

１．処理者は、別紙１のF行に記載された他の第三者（以下「復処理者」といいます。）及び、該当する場合には、処理者がウェブサイトに公開する復処理者リストに記載された復処理者を選任することについて、管理者の一般的な承認（general　authorization）を得たものとします。処理者は、管理者に対し、復処理者の追加又は変更を行う場合は、当該変更に伴う一覧の変更予定を通知しなければなりません。当該通知の際、処理者は、管理者が異議を申し立てる権利を行使するために必要な情報（復処理者の名称を含む）を提供します。管理者は、復処理者の起用について、処理者から当該別の処理者の起用に関する通知を受けた日から１０営業日以内に、書面による異議を申し立てることができます。
２．管理者のための特定の処理活動を行うために処理者が復処理者を業務に従事させる場合、当該復処理者に対し、契約又は他の法律行為によって、本DPAに定められたデータ保護義務を下回らないデータ保護上の義務を課さなければなりません。当該復処理者がそのデータ保護の義務を充足しない場合、処理者は当該復処理者の義務の履行について管理者に対する責任を全面的に負うものとします。
３．復処理者の専任が越境データ移転をひき起こす場合、処理者は、適用されるデータ保護法に基づく越境データ移転を規律する規制を遵守するための必要な措置を講じます。
４．別紙１のF行及び処理者がウェブサイトに公開する復処理者リストに記載された復処理者は、個人データの処理に従事することができます。処理者は、復処理者を慎重に、特に、これが講じる技術的・組織的措置の適切さを考慮した上で選択したことを表明します。管理者は、本条第２項乃至本条第４項に従うことを条件に、かかる復処理者の使用を承認します。

第６条 処理者の権限の下における処理

処理者は、その権限の下で行動する者であって、個人データにアクセス可能な者は、本DPAまたはサービス規約に定められている管理者からの指示によらない限り当該個人データを処理しないことを確保しなければなりません。但し、適用されるデータ保護法により処理が義務付けられる場合を除きます。

第７条 特定の技術的・組織的措置

１．処理者は、データ処理により生じるリスクに対して適切な水準の安全性を確保するための技術上及び組織上の措置を実施しなければなりません。かかる措置には、例えば以下のような事項が含まれ得るものとします。

（ａ）　個人データの仮名化又は暗号化
（ｂ）　処理のシステム及び本サービスの機密性、完全性、可用性及び回復可能性の確保
（ｃ）　物理的又は技術的な事故が発生した際に、適時に個人データの可用性及び個人データへのアクセスを復旧する能力の確保
（ｄ）　処理の安全性を確保するための技術上及び組織上の措置の有効性の定期的なテスト、評価等の手順策定と実施

２．処理者が前項に関して実施する技術上及び組織上の措置は、別紙２記載のとおりとします。

３．技術的・組織的措置は、技術の発展及び改良に応じて変更されます。したがって、処理者は、これらの措置が適切な水準の安全性を提供し続けることを確保するために、定期的な確認を実施し、必要に応じて、別紙２に定める措置に加えて追加の又は別の措置を講じるものとします。

４．処理者は、実施した技術的・組織的措置を管理者に証明するため、その裁量において、独立の組織（例えば、監査人、内部監査人、データ保護責任者、ＩＴセキュリティ部門、データ保護監査人、品質監査人）による認証書、報告書若しくは報告書の抜粋又はＩＴセキュリティ部門若しくはデータ保護監査人による適切な証明書を提出することができます。

５．前第１項乃至第４項に記載の特定の技術的・組織的措置に加え、処理者は、物理的及び人的観点からの安全措置を講じ、必要に応じて継続的に改善するものとします。

６．処理者は、管理者から書面による要請があった場合には、当該管理者に対して、処理者の義務に関して、当該要請に回答するに必要な情報を提供するものとします。処理者は、監督機関又は管理者から適用される法令上義務付けられた検査を求められた場合には、これに誠実に合理的な協力を行うものとします。

別紙１

本DPAに基づく個人データの処理の内容

A	**処理の性質及び目的（Nature and purposes of the processing）**	• 処理者と管理者との間で合意された本サービスを提供すること • 本サービスの利用状況の監視と分析を通じて、サービスパフォーマンスを最適化し、信頼性を向上させること • 処理者が本サービスの提供にあたり保守上、運用上または技術上必要であると判断した場合、テナントデータについて、監視、分析、調査等必要な行為を行うこと 以下は、Tadrill利用者に適用されます。 • 標的型攻撃メールに関する報告の内容の確認及び分析を行うこと • お客様に提供するための標的型攻撃メール訓練サービス対象者リストを作成すること。処理者は、アクセスした情報を第三者に提供又は開示しないものとします。
B	**処理の対象（Subject matter of the processing）**	• サービスおよびサービスを介した他のクラウドサービスにアクセスする際の認証および承認に関連するデータ。 • 管理者のシステムおよびユーザーによって送受信されるEメール、添付ファイル、共有ファイルの内容およびメタデータ • 本サービスの使用を通じて生成されるシステムログ、イベントログ、および監査ログ。 以下はTadrill利用者に適用されます。 Google LLCが提供するGmailのような第三者サービスに含まれる個人データ。これには、送信者および受信者（CCおよびBCCを含む）の氏名とメールアドレス、ヘッダー、件名、本文などのメール内容、Tadrill利用者の氏名、メールアドレス、所属組織単位などのユーザー情報が含まれます。
C	**データ主体の類型（Categories of the Data Subjects）**	• 管理者の従業員や委託先などの内部関係者 • 管理者の外部関係者
D	**個人データの種類（Type of Personal Data）**	• 識別、認証、連絡先情報 o 氏名、メールアドレス、アドミン管理者が入力したその他の関連情報 • 通信およびコンテンツ情報 o Eメール、添付ファイル、ファイル • セキュリティ及び運用関連情報 o アクセスログ、監査ログ、アクションログなど • IPアドレス

		• トラッキングID (amplitude, Google Analytics) • デバイス ID • MAC アドレス • クッキー使用によって取得されるその他の情報
E	**処理の期間（Duration of processing）**	別途定めがない限り、データ処理は管理者への本サービス提供が終了または期間満了となった時点で停止されるものとします。
F	**復処理者（Sub-processor）**	1. **アマゾン ウェブ サービス ジャパン合同会社** a. 〒141-0021 東京都品川区上大崎3-1-1 2. **Datadog, Inc.** a. 620 8th Ave 45th Floor, New York, NY 10018 USA 3. **Functional Software, Inc. doing business as Sentry** a. 45 Fremont Street, 8th Floor, San Francisco, CA 94105 USA 4. **Salesforce** a. 〒100-0005 東京都千代田区丸の内1-1-3 Salesforce Tower 5. **Hubspot** a. 2 Canal Park, Cambridge, MA 02141, United States 6. **Zendesk** a. San Francisco, California, USA (specifically, 181 S. Fremont Street, San Francisco, CA 94105) 7. **Statuspage** a. Level 6, 341 George Street, Sydney, NSW 2000, Australia 8. **WithSecure K.K.** a. 〒100-0004 東京都千代田区大手町1-7-2 東京サンケイビル27 9. **Cybertrust** a. 〒105-0001 東京都港区虎ノ門1-2-8 虎ノ門琴平タワー 10. **ngrok** a. 548 Market St PMB 26741, San Francisco, CA USA 11. **Anyflow** a. 〒150-0002 東京都渋谷区渋谷3-26-16 第5叶ビル5F

別紙2

技術的及び組織的措置

1. 建物や施設へのアクセスコントロール

個人データを管理する建物や施設への権限なき物理的アクセスを阻止するために、以下を含む措置を講じる。

- アクセスコントロールシステム
- IDリーダー、磁気カード、ICチップカード、社給スマートフォン
- ドアの施錠
- 監視システム
- 警報システム、ビデオ・テレビモニター
- 施設への入退場時のログの記録

2. システムへのアクセスコントロール

ITシステムへの権限なきアクセスを阻止するために、ユーザー認識及び認証を含む下記の措置を講じる。

- パスワード（特殊文字の使用、最低文字数の制限、定期的な変更を含む）
- ゲストユーザーや匿名アカウントによるアクセスの遮断
- システムへの HENNGE Access Control を経由したアクセスの集中管理
- IT部門による承認に基づくITシステムへのアクセス

3. データへのアクセスコントロール

権限あるユーザーが与えられた権限を越えてデータにアクセスすることを防ぐために、以下を含む措置を講じる。

- アクセス権限の区別
- 職務内容に応じて定義されたアクセス権限
- HENNGE Access Control 経由のユーザーアクセスログの自動的記録

4. データ移転時のコントロール

データ移転が行われる際に権限なきアクセス又はデータの変更若しくは削除が行われることを阻止し、移転が安全に行われ、記録されていることを確保するために、以下を含む措置を講じる。

- データ移転については HENNGE Email DLP やHENNGE Secure Transfer 及び、HENNGE Secure Download が使用されるようにすること
- https通信を必須としたリモートアクセス、データの移転及び通信については HENNGE Access Control を利用して暗号化すること

5. 入力等のコントロール

データの管理・維持の内容を記録し、データの修正・削除が行われたこと及び誰によってそれがなされたかについて確認することができるように、以下を含む措置を講じる。

・ 自社導入している HENNGE One 各種サービス上でのユーザー操作の記録

6. 業務のコントロール

処理者の指示に厳密に基づいてデータの処理が行われるようにするために、以下を含む措置を講じる。

・ ISMS 27001 及び ISO27018 認証資格に基づく明確な文章による契約に基づく指示

・ 契約の履行状況についての監視

7. 可用性のコントロール

偶発的なデータの損壊や紛失からデータを保護するために、以下を含む措置を講じる。

・ バックアップ

・ 停電に備えた電源装置

・ 事業継続計画

・ 遠隔記憶装置

・ アンチウイルスシステム又はファイアウォールシステム

8. 分離のコントロール

異なる目的で取得したデータを分離して処理するために、以下を含む措置を講じる。

・ スタッフの業務内容に応じて、異なる目的で保存されるデータへのアクセスを制限すること

・ HENNGE Access Control による各業務用ITシステムへのアクセス権の分離

・ ITテスト及び生産環境の分離