The Japanese version is for reference purposes and the English version prevails.

日本語版は参考であり、英文版が優先する。

Staffbase Data Processing Agreement		Staffbaseデータ処理契約	
1	**INTRODUCTION**	**1**	序文
(a)	This Data Processing Agreement ("**DPA**") is incorporated into, and is subject to the terms and conditions of the Master Subscription Agreement or other agreement agreed between Staffbase and Customer governing Customer's use of the Services (the "**Agreement**"). Any capitalized term used but not defined in this DPA shall have the meaning given to it in the Agreement.	(a)	本データ処理契約(以下「**DPA**」という。)は、マスターサブスクリプション契約、又は顧客による本件サービスの利用に適用されるStaffbaseと顧客との間のその他の契約(以下「本契約」という。)に組み入れられ、その条件の適用を受ける。本DPAにおいて定義されていない用語は、本契約において付与された意味を有する。
(b)	The parties agree that this DPA replaces and supersedes any existing DPA the parties may have previously entered into in connection with the Services.	(b)	両当事者は、本DPAが、本件サービスに関連して両当事者間で過去に締結された既存のDPAに置き換わり、これに優先することに合意する。
(c)	Customer and Staffbase acknowledge that any exclusions or limitations of liability in the Agreement do not limit the liability of either party with respect to claims brought by Data Subjects under Data Protection Laws.	(c)	顧客及びStaffbaseは、本契約における責任の除外又は制限によって、データ保護法に基づいてデータ主体が申し立てる請求に関するいずれの当事者の責任も、制限されないことを認める。
(d)	The DPA shall prevail if there is a conflict between the Agreement and the DPA.	(d)	本契約とDPAの間で矛盾がある場合、DPAが優先するものとする。
(e)	This DPA uses the 'processor-controller' standard contractual clauses published by the European Commission for the purpose of Article 28(3) GDPR (Implementing Decision (EU) 2021/915 of 4 June 2021) (the "**Clauses**") with minimal deviations to reflect Staffbase's processes and our global business.	(e)	本DPAは、Staffbaseのプロセス及びグローバル事業を反映させた最低限の逸脱を除き、GDPR第28条第(3)項(2021年6月4日欧州委員会実施決定(EU)2021/915)を目的として欧州委員会が発行した「処理者・管理者」標準契約条項(以下「本条項」という。)を使用する。
2	**DEFINITIONS** "**Australian Privacy Laws**" has the meaning given in the Australian Privacy Law Addendum found at: https://staffbase.com/en/legal/. Only to the extent that Staffbase processes Personal Data governed by Australian Privacy Laws, will the Australian Privacy Law Addendum apply in addition to the terms of this DPA. "**Canadian Privacy Laws**" means the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), Quebec Law 25, and any other federal or provincial legislation or regulations in Canada related to Personal Data. "**Data Protection Laws**" means, to the extent applicable: **(i)** European Data Protection Law, **(ii)** US Privacy Laws, **(iii)** Canadian Privacy Laws, and **(iv)** Australian Privacy Laws. "**European Data Protection Law**" means: **(i)** the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**"); **(ii)** applicable national implementations of the GDPR in the European Union ("**EU**") and European Economic Area ("**EEA**") member states; **(iii)** in respect of the United Kingdom ("**UK**"), the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK Data Protection Law**"); **(iv)** EU ePrivacy Directive 2002/58/EC; as amended by	**2**	定義 「オーストラリアプライバシー法」は、https://staffbase.com/en/legal/に掲載するオーストラリアプライバシー法補遺で付与する意味を有する。Staffbaseがオーストラリアプライバシー法の適用を受ける個人データを処理する範囲内においてのみ、本DPAの条件に加えてオーストラリアプライバシー法補遺が適用される。 「カナダプライバシー法」とは、個人情報保護及び電子文書法(S.C.2000, c.5)、ケベック州法第25号及びその他個人情報に関するカナダの連邦又は州の法律若しくは規則を意味する。 「データ保護法」とは、適用される範囲において、**(i)**欧州データ保護法、**(ii)**米国プライバシー法、**(iii)**カナダプライバシー法及び**(iv)**オーストラリアプライバシー法を意味する。 「欧州データ保護法」とは、**(i)**一般データ保護規則((EU)2016/679)(以下「**GDPR**」という。)、**(ii)**欧州連合(以下「**EU**」という。)及び欧州経済領域(以下「**EEA**」という。)の加盟国における適用あるGDPR国内実施規則、**(iii)**英国(以下「英国」という。)における2018年データ保護法及び英国の2018年欧州連合(離脱)法第3条により英国法の一部として保存されたGDPR(以下「英国データ保護法」という。)、(iv) EU eプライバシー指令2002/58/EC(指令2009/136/ECによる改正を含む。)、並びに(v)2020年9月25日スイス連邦データ保護法及びその施行規則(随時の改正、優先又は置換を含む。以下「**FADP**」という。)を意味する。 「モデル条項」とは、欧州データ保護法が適用される場合の、2021年6月4日欧州委員会実施決定(EU)2021/914で

Staffbase

Directive 2009/136/EC; and **(v)** Swiss Federal Act on Data Protection of 25 September 2020 and its implementing regulations as amended, superseded, or replaced from time to time ("**FADP**"). "**Model Clauses**" means, where European Data Protection Law applies, Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (currently found at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj), as may be amended or superseded from time to time. "**Personal Data**" means any information relating to an identified or identifiable natural person where **(i)** such information is contained in Customer Content; and **(ii)** is protected similarly as personal data, personal information, personal identifiable information under applicable Data Protection Law. "**Personal Data Breach**" means a breach of security that has resulted in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by Staffbase and/or its Sub-Processors in connection with the provision of the Services. "**Restricted Transfer**" means, where European Data Protection Law applies, a transfer of Personal Data to a Third Country. "**Sub-Processor**" means any Processor engaged by Staffbase or its Affiliates to assist in fulfilling Staffbase's obligations under the Agreement. Sub-Processors may include third parties or Staffbase Affiliates. "**Third Country**" means **(a)** to the extent the GDPR applies to the processing of Personal Data by Staffbase, a country outside of the EEA which is not subject to an adequacy decision by the European Commission; **(b)** to the extent the UK Data Protection Law applies to the processing of Personal Data by Staffbase, country which is not subject to an adequacy decision pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and **(c)** to the extent the FADP applies to the processing of Personal Data by Staffbase, a country outside the EEA and/or Switzerland not subject to an adequacy decision by the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**"). "**UK Addendum**" means the International Data Transfer Addendum issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018 (currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf), as may be amended or superseded from time to time. "**US Privacy Laws**" has the meaning given in the US State Privacy Law Addendum. "**US State Privacy Law Addendum**" means the US State privacy law addendum found at:	承認された欧州議会及び理事会規則(EU)2016/679(現在https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj に掲載。)に従った個人データの第三国への移転に関する標準契約条項(随時の改正及び置換を含む。)を意味する。 「個人データ」とは、特定された、又は特定可能な自然人に関連する情報であって、**(i)**顧客コンテンツに含まれるもの、及び、**(ii)**適用あるデータ保護法に基づいて個人のデータ、個人の情報、個人が特定可能な情報と同様に保護されるものを意味する。 「個人データ侵害」とは、本件サービスの提供に関連してStaffbase及び/又はその復処理者が送信、保管又はその他の処理を行う個人データについて、事故により又は違法に破壊、喪失、変更、不正開示、又はアクセスされる結果となったセキュリティの侵害を意味する。 「制限対象移転」とは、欧州データ保護法が適用される場合において、第三国への個人データへの移転を意味する。 「復処理者」とは、本契約に基づくStaffbaseの義務の履行の支援を受けるためにStaffbase又はその関連会社が起用する処理者を意味する。復処理者には、第三者又はStaffbaseの関連会社を含めることができる。 「第三国」とは、以下を意味する。**(a)**Staffbaseによる個人データの処理にGDPRが適用される範囲の、欧州委員会による十分性認定の対象でないEEA域外の国。 **(b)**Staffbaseによる個人データの処理に英国データ保護法が適用される範囲の、2018年英国データ保護法第17条第A項に従った十分性認定の対象でない国。並びに、 **(c)**Staffbaseによる個人データの処理にFADPが適用される範囲の、スイス連邦データ保護情報コミッショナー(以下「**FDPIC**」という。)による十分性認定の対象でないEEA域外及び/又はスイス域外の国。 「英国補遺」とは、2018年英国データ保護法第119条第(A)項に基づいて情報コミッショナーオフィスが発行した国際間データ移転に関する補遺(現在 https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdfに掲載。)(随時の改正及び置換を含む。)を意味する。 「米国プライバシー法」は、米国州プライバシー法補遺において与えられる意味を有する。 「米国州プライバシー法補遺」とは、https://staffbase.com/en/legal/に掲載する米国州プライバシー法補遺を意味する。米国プライバシー法が適用される個人データをStaffbaseが処理する範囲内において、本DPAの条件に加え、米国州プライバシー法補遺が適用される。 「管理者」、「データ主体」、「処理者」及び「処理」という用語は、データ保護法に基づいて与えられる意味を有し、「処理する」及び「処理される」は、これに従って解釈される。ここに明示的に定義されていないその他の用語は、本契約における意味と同じ意味を有する。

https://staffbase.com/en/legal/. To the extent that Staffbase processes Personal Data governed by US Privacy Laws, will the US State Privacy Laws Addendum apply in addition to the terms of this DPA. The terms "**Controller**", "**Data Subject**", "**Processor**" and "**processing**" shall have the meaning given to them under Data Protection Law and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly. Any other terms not expressly defined here have the same meanings as in the Agreement.	
3 THE CLAUSES **Clause 1 - Purpose and scope** (a) The purpose of this DPA is to ensure compliance with Data Protection Laws as they may be amended, replaced or supplemented from time to time. (b) Staffbase and Customer have agreed to this DPA in order to ensure compliance with Data Protection Laws. (c) This DPA applies to the processing of Personal Data as specified in Annex II. (d) The Annexes are an integral part of this DPA. (e) This DPA is without prejudice to obligations to which Customer is subject by virtue of Data Protection Law. (f) This DPA does not by itself ensure compliance with obligations related to international transfers in accordance with Data Protection Laws, where applicable.	**3 条項** **第1条 - 目的及び範囲** (a) 本DPAの目的は、随時改正、置換又は補完されるデータ保護法への準拠を徹底することにある。 (b) Staffbase及び顧客は、データ保護法への準拠を徹底するため、本DPAに合意した。 (c) 本DPAは、附属書IIに記載のある個人データの処理に適用される。 (d) 各附属書は本DPAの不可分の一部である。 (e) 本DPAにより、データ保護法を理由として顧客に課される義務が損なわれることはない。 (f) 本DPAは、(該当する場合)それ自体が単独で、データ保護法に従う国際間移転に関連する義務の遵守を確保するものではない。
Clause 2 – Invariability of the Clauses [Not applicable]	***第2条 – 条項の不変性 [該当しない]***
Clause 3 - Interpretation (a) Where this DPA uses any terms as defined in Data Protection Laws, those terms shall have the same meaning as in the applicable Data Protection Law. (b) This DPA shall be read and interpreted in the light of the provisions of the Data Protections Laws, to the extent that they apply. (c) This DPA shall not be interpreted in a way that runs counter to the rights and obligations provided for in the Data Protection Laws or in a way that prejudices the fundamental rights or freedoms of the Data Subjects.	**第3条 - 解釈** (a) 本DPAにおいてデータ保護法で定義される用語を使用する場合、それらの用語は適用あるデータ保護法と同じ意味を有する。 (b) 本DPAは、データ保護法が適用される範囲内において、データ保護法の規定に照らして理解され解釈される。 (c) 本DPAを、データ保護法が規定する権利及び義務に反する形で、又はデータ主体の基本的権利又は自由を損なう形で解釈してはならない。
Clause 4 - Hierarchy In the event of a contradiction between this DPA and the provisions of related agreements between the parties existing at the time when this DPA is agreed or entered into thereafter, this DPA shall prevail.	**第4条 - 優先順位** 本DPAと、本DPAが合意された時点又はその後に締結された時点で存在する両当事者間の関連する合意の規定との間に矛盾がある場合、本DPAが優先するものとする。
Clause 5 - Docking clause [Not applicable]	***第5条 - ドッキング条項 [該当しない]***
Clause 6 - Description of processing(s) The details of the processing operations, in particular the categories of Personal Data and the purposes of processing for which the Personal Data is processed on behalf of Customer, are specified in Annex II.	**第6条 - 処理の概要** 処理手順の詳細、特に個人データのカテゴリー、及び顧客に代わって個人データを処理する目的は、附属書IIに定める。
Clause 7 - Obligations of the Parties **7.1 Instructions** (a) Staffbase shall process Personal Data only on documented instructions from Customer, unless required to do so by local law to which Staffbase is subject, such as EU or EU Member State law. In this case, Staffbase shall inform Customer of that legal	**第7条 - 当事者の義務** **7.1 指示** (a) Staffbaseは、顧客から文書化された指示がある場合にのみ、個人データを処理する。但し、EU法又はEU加盟国法等、Staffbaseが適用対象である現地法により処理が義務づけられる場合は、その限りではない。そのような場合、Staffbaseは処理の前に当該法的義務について顧客に連

requirement before processing, unless the law prohibits this. The Agreement (including this DPA), any applicable Order Form(s), together with the use of the Services, constitute Customer's complete instructions to Staffbase for the processing of Personal Data. Subsequent instructions may also be given by Customer throughout the duration of the processing of Personal Data as long as they are consistent with the terms of this DPA and the Agreement. These instructions shall always be documented.

(b) Staffbase shall immediately inform Customer if, in Staffbase's opinion, instructions given by Customer infringe Data Protection Laws.

7.2 Purpose limitation

Staffbase shall process the Personal Data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from Customer.

7.3 Duration of the processing of Personal Data

Processing by Staffbase shall only take place for the duration specified in Annex II.

7.4 Security of processing

(a) Staffbase shall at least implement the technical and organizational measures specified in Annex III to ensure the security of the Personal Data. This includes protecting the data against a Personal Data Breach. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the Data Subjects.

(b) Staffbase shall grant access to the Personal Data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Agreement. Staffbase shall ensure that persons authorized to process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

If the processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offenses ("**Sensitive Data**"), Staffbase shall apply specific restrictions and/or additional safeguards where possible and when required under Data Protection Law. Customer controls whether they process any Sensitive Data in relation with the Staffbase Services and Customer must ensure compliance with Data Protection Laws when processing Sensitive Data.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with this DPA.

(b) Staffbase shall deal promptly and adequately with inquiries from Customer about the processing of Personal Data in accordance with this DPA.

(c) Staffbase shall make available to Customer all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from Data Protection Laws. At

絡するものとするが、法によりこれが禁止されている場合は、その限りではない。本契約(本DPAを含む。)及び該当する本件注文書は、本件サービスの利用と併せて、個人データの処理に関する顧客からStaffbaseへの完全な指示を構成する。顧客は、その後も個人データ処理が継続する間、本DPA及び本契約の規定と整合する内容である限り、後続の指示を行うことができる。これらの指示は、必ず文書化するものとする。

(b) 顧客が与える指示が、Staffbaseの意見においてデータ保護法に抵触すると判断される場合、Staffbaseは直ちに顧客に知らせるものとする。

7.2 目的の制限

Staffbaseは、附属書IIに定める特定の処理の目的のためにのみ、個人データを処理する。但し、顧客から追加指示を受領した場合は、その限りではない。

7.3 個人データの処理期間

Staffbaseによる処理は、附属書IIに定める期間にのみ行われるものとする。

7.4 処理のセキュリティ

(a) Staffbaseは、個人データのセキュリティを確保するため、少なくとも附属書IIIに定める技術的及び組織的な対策を講じる。これには、個人データ侵害に対するデータ保護策が含まれる。適切な水準のセキュリティを検討する際に、両当事者は、最新技術、実施コスト、処理の性質、範囲、背景及び目的、並びにデータ主体へのリスクを十分に考慮するものとする。

(b) Staffbaseは、本契約の実施、管理、監視のために厳格に必要な範囲でのみ、その人員に処理対象の個人データへのアクセスを許可する。Staffbaseは、個人データの処理を許可された者が守秘義務を確約するか、又は適切な法律上の守秘義務の適用対象であるよう徹底する。

7.5 センシティブデータ

処理において、人種的若しくは民族的出自、政治的見解、宗教的若しくは哲学的信条、又は労働組合の加入状況、遺伝子データ若しくは自然人を一意に特定する目的の生体認証データ、健康状態又は人の性生活若しくは性的指向に関するデータ、又は有罪判決及び犯罪歴に関連するデータを明らかにする個人データ(以下「センシティブデータ」という。)を取り扱う場合、Staffbaseは、可能な限り、かつデータ保護法により義務づけられる場合、具体的な制限及び/又は追加の保護手段を適用するものとする。顧客は、Staffbaseの本件サービスに関連してセンシティブデータの処理を行うか否かを管理し、センシティブデータの処理においてデータ保護法が遵守されるよう徹底しなければならない。

7.6 文書化及び遵守

(a) 両当事者は、本DPAの遵守を証明できなければならない。

(b) Staffbaseは、本DPAに従った個人データの処理に関する顧客からの問い合わせに、速やかにかつ十分に対応する。

(c) Staffbaseは、本DPAに定めのある、データ保護法から直接生じる義務の遵守を証明するため、必要となる全ての情報を顧客に提供する。また、顧客の要請があれば、Staffbaseは、合理的な間隔で、又は非準拠の兆候がある場合に、本DPAの対象となる処理活動の監査を許可し、それに協力する。顧客は、検査又は監査を判断する際に、Staffbaseが保持する関連認証を考慮に入れることができる。

(d) 顧客は、監査を自ら実施するか、又は独立した監査人を任命するかを選択できる。監査には、相互の合意があればStaffbaseの事業所又は物理的施設での検査を含めることもでき、適切な場合、合理的な事前通知をもって実施するものとする。

(e) 両当事者は、本条に言及のある情報(監査の結果を含む。)を、要求に応じて管轄監督機関(複数の場合を含む。)に提供するものとする。

Customer's request, Staffbase shall also permit and contribute to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, Customer may take into account relevant certifications held by Staffbase.	
(d) Customer may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of Staffbase if mutually agreed and shall, where appropriate, be carried out with reasonable notice.	
(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.	
7.7 Use of sub-processors	**7.7** 復処理者の使用
(a) Staffbase has Customer's general authorisation for the engagement of Sub-Processors listed at https://staffbase.com/en/legal/subprocessors/. Staffbase shall specifically inform in writing Customer of any intended changes of that list through the addition or replacement of Sub-Processors at least 30 days in advance, thereby giving Customer sufficient time to be able to object, to such changes, solely based on reasonable data protection grounds related to the protection of the Personal Data, prior to the engagement of the concerned Sub-Processor(s). Staffbase shall provide Customer with the information necessary to enable Customer to exercise the right to object. Customer's notice shall contain the grounds for the objection. The Parties shall discuss Customer's concerns in good faith with the intention of achieving a commercially reasonable solution. If Parties are not able to find a solution, Staffbase and Customer each have the right to terminate the Agreement, including any related Order, with 30 days' notice and without liability to either party.	(a) Staffbaseは、https://staffbase.com/en/legal/subprocessors/のリストに示す復処理者の起用に関して、顧客の一般的許可を有する。Staffbaseは、復処理者の追加又は交代によりこのリストを変更する場合、少なくとも30日前にその意図を顧客に書面で明示的に通知し、当該復処理者が起用される前に、変更に異議を唱えるに十分な時間を顧客に与えるものとするが、この異議は、個人データ保護に関する合理的なデータ保護の理由に基づいてのみ申立てるものとする。Staffbaseは顧客に対し、顧客が異議を唱える権利を行使するために必要な情報を提供する。顧客の通知には、異議申立の理由を記載するものとする。両当事者は、商業的に合理的な解決策に至ることを意図し、誠意をもって顧客の懸念を協議する。両当事者が解決策を見出すことができない場合、Staffbase及び顧客はそれぞれ、30日前の通知をもって他方当事者に対する責任を生じることなく、本契約（関連する本件注文書を含む。）を解除する権利を有するものとする。
(b) Where Staffbase engages a Sub-Processor for carrying out specific processing activities (on behalf of Customer), it shall do so by way of a contract which imposes on the Sub-Processor, in substance, the same data protection obligations as the ones imposed on Staffbase in accordance with this DPA. Staffbase shall ensure that the Sub-Processor complies with the obligations to which Staffbase is subject pursuant to this DPA and applicable Data Protection Law.	(b) Staffbaseが特定の処理活動を（顧客に代わって）行うための復処理者を起用する場合、本DPAに従い、Staffbaseに課されるデータ保護義務と実質的に同じ義務を復処理者に対して課す契約をもって行うものとする。Staffbaseは、復処理者が本DPA及び適用あるデータ保護法に従ってStaffbaseに課される義務を遵守するよう徹底する。
(c) At Customer's request, Staffbase shall provide a copy of such a Sub-Processor agreement and any subsequent amendments to Customer. To the extent necessary to protect business secrets or other confidential information, including Personal Data, Staffbase may redact the text of the agreement prior to sharing the copy.	(c) 顧客の要請があれば、Staffbaseは、復処理者との契約及びその後の変更の写しを顧客に提供する。Staffbaseは、企業秘密又はその他の機密情報（個人データを含む。）を保護するために必要な範囲で、写しを提供する前に、契約書の文面を墨消しにすることができる。
(d) Staffbase shall remain fully responsible to Customer for the performance of the Sub-Processor's obligations in accordance with its contract with Staffbase. Staffbase shall notify Customer of any material failure by the Sub-Processor to fulfill its contractual obligations to process Customer's Personal Data in accordance with this DPA.	(d) Staffbaseは、Staffbaseとの契約に従った復処理者の義務の履行について、顧客に対し全ての責任を負う。本DPAに従って顧客の個人データを処理する契約上の義務について、復処理者による重大な不履行があった場合、Staffbaseは顧客に通知する。
	(e) *[第7条第7項第(e)号は意図的に削除]*
	7.8 国際間移転
	(a) Staffbaseが個人データを第三国又は国際機関に移転する場合、文書化された顧客の指示によるか、又はStaffbaseに適用される現地法の特定の義務を履行するためにのみ行うものとし、（該当する場合）データ保護法に準拠して行う。Staffbaseは、第7条第7項の通知義務を条件として、個人データを、第三国に所在する自己の関連会社又は復処理者に移転することができる。
	(b) 顧客は、Staffbaseが（顧客に代わって）特定の処理活動を行うために第7条第7項に従って復処理者を起用し、その処理活動において個人データが直接又は間接的に第三国に移転される場合に、Staffbase及び当該復処理者が、モデル条項を使用して、欧州データ保護法、及び、該当する場合は英国補遺への準拠を確保することができることに同意する。但し、当該モデル条項の使用に関する条件を満たさなければならない。
	(c) 顧客からStaffbaseへの個人データの移転が制限対象移転に該当し、欧州データ保護法により適切な保護手段を講じることが義務づけられる場合、当該移転はモデル条項の対象となり、モデル条項は附属書V（モデル条項）に従って本DPAに組み入れられ、その不可分の一部をなすとみなされる。

(e) *[Clause 7.7(e) is intentionally deleted]* **7.8 International transfers** (a) Any transfer of Personal Data to a Third Country or to an international organization by Staffbase shall be done only on the basis of documented instructions from Customer or in order to fulfill a specific requirement under local law to which Staffbase is subject and shall take place in compliance with Data Protection Law (as applicable). Staffbase may transfer Personal Data to its Affiliates or its Sub-Processors located in a Third Country, subject to the notification requirements of Clause 7.7. (b) Customer agrees that where Staffbase engages a Sub-Processor in accordance with Clause 7.7 for carrying out specific processing activities (on behalf of Customer) and those processing activities involve a transfer of Personal Data, either directly or indirectly, to any Third Country, Staffbase and the Sub-Processor can ensure compliance with European Data Protection Law by using the Model Clauses and, where relevant, the UK Addendum, provided the conditions for the use of those Model Clauses are met. (c) When the transfer of Personal Data from Customer to Staffbase qualifies as a Restricted Transfer, and European Data Protection Law requires that appropriate safeguards are put in place, the transfer shall be subject to Model Clauses which shall be deemed incorporated into and form an integral part of this DPA in accordance with Annex V (Model Clauses).	
Clause 8 - Assistance to Customer (a) Staffbase shall promptly notify Customer of any request it has received from the Data Subject **("Data Subject Request**"). It shall not respond to the request itself, unless authorized to do so by Customer. (b) Staffbase shall assist Customer in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), Staffbase shall comply with Customer's instructions. (c) In addition to Staffbase's obligation to assist Customer pursuant to Clause 8(b), Staffbase shall furthermore assist Customer in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to Staffbase: (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons; (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by Customer to mitigate the risk;	第8条 - 顧客への支援 (a) Staffbaseは、データ主体から受領した要請（以下「データ主体の要請」という。）について、速やかに顧客に通知する。Staffbaseは、顧客から許可された場合を除き、自ら要請に対応してはならない。 (b) Staffbaseは、処理の性質を考慮して、顧客がデータ主体による権利行使の要請に対応する自己の義務を履行できるよう支援する。(a)及び(b)に従って義務を履行する際、Staffbaseは、顧客の指示に従う。 (c) Staffbaseの第8条第(b)項に従った顧客を支援する義務に加え、Staffbaseはさらに、データ処理の性質及びStaffbaseが入手できる情報を考慮して、顧客が以下の義務の遵守を徹底できるよう支援する。 (1) 処理の種類により、自然人の権利及び自由に対し高リスクを生じる可能性が高い場合、企図される処理業務が個人データ保護に与える影響を評価する（以下「データ保護影響評価」という。）義務。 (2) データ保護影響評価で、顧客がリスク低減策を講じなければ処理の結果高いリスクが生じることが示唆される場合、処理前に管轄監督機関（複数の場合を含む。）に相談する義務。 (3) 処理中の個人データが不正確又は古いとStaffbaseが気づいた場合、遅滞なく顧客に連絡し、個人データが正確で最新のものであるよう徹底する義務。 (4) データ保護法に定める義務。 (d) 両当事者は、Staffbaseが本条項の適用について顧客を支援するために必要な適切な技術的・組織的対策、及び、必要な支援の範囲と程度を、附属書IIIに規定する。

(3) the obligation to ensure that Personal Data is accurate and up to date, by informing Customer without delay if Staffbase becomes aware that the Personal Data it is processing is inaccurate or has become outdated; (4) the obligations in Data Protection Laws. (d) The Parties shall set out in Annex III the appropriate technical and organizational measures by which Staffbase is required to assist Customer in the application of this Clause as well as the scope and the extent of the assistance required.	
Clause 9 - Notification of Personal Data Breach In the event of a Personal Data Breach, Staffbase shall cooperate with and assist Customer for Customer to comply with its obligations under Data Protection Laws, where applicable, taking into account the nature of processing and the information available to Staffbase. **9.1 Data breach concerning data processed by Customer** In the event of a Personal Data Breach concerning Personal Data processed by Customer, Staffbase shall assist Customer: (a) in notifying the Personal Data Breach to the competent supervisory authority/ies, without undue delay after Customer has become aware of it, where relevant (unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons); (b) in obtaining the following information which, pursuant to Data Protection Laws, shall be stated in Customer's notification, and must at least include: (1) the nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (2) the likely consequences of the Personal Data Breach; (3) the measures taken or proposed to be taken by Customer to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay. (c) in complying, pursuant to Data Protection Laws, with the obligation to communicate without undue delay the Personal Data Breach to the Data Subject, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons. **9.2 Data breach concerning data processed by Staffbase** In the event of a Personal Data Breach concerning Customer's Personal Data processed by Staffbase in relation to the Services, Staffbase shall notify Customer without undue delay after Staffbase having become aware of the Personal Data Breach. Such notification shall	第9条 - 個人データ侵害の通知 個人データ侵害が発生した場合、Staffbaseは、データ処理の性質及びStaffbaseが入手できる情報を考慮して、該当する場合、顧客がデータ保護法に基づく義務を履行できるよう顧客と協力し、支援を行う。 **9.1** 顧客が処理するデータに関するデータ侵害 顧客が処理する個人データに関する個人データ侵害が発生した場合、Staffbaseは、以下について顧客を支援する。 (a) 該当する場合、顧客が個人データ侵害に気づいた後、不当な遅滞なく管轄監督機関(複数の場合を含む。)に個人データ侵害を通知すること(但し、当該個人データ侵害が自然人の権利及び自由にリスクを及ぼす可能性が低い場合は、その限りではない)。 (b) 以下の情報を取得すること。この情報は、データ保護法に従って顧客への通知に記載し、少なくとも以下を含むものとする。 (1) 個人データの性質。これには、可能な限り、関係するデータ主体のカテゴリーと概数及び関係する個人データ記録のカテゴリーと概数を含む。 (2) 当該個人テ゛ータ侵害によって発生する可能性のある影響。 (3) 顧客が当該個人データ侵害に対応するために取った、又は取ることが予定される措置(適切な場合には、生じる可能性のある悪影響を軽減するための措置を含む。)。 これらの情報の全てを同時に提供することが不可能である場合に限り、最初の通知にはその時点で入手可能な情報を記載するものとし、それ以上の情報は、入手可能となるに従って、後日不当な遅滞なく提供する。 (c) 個人データ侵害が自然人の権利及び自由に対し高リスクをもたらす可能性が高い場合、データ保護法に従って、個人データ侵害について不当な遅滞なくデータ主体に知らせる義務を遵守すること。 **9.2 Staffbase**が処理するデータに関するデータ侵害 本件サービスに関連して、Staffbaseが処理する顧客の個人データに関する個人データ侵害が発生した場合、Staffbaseは、Staffbaseが個人データ侵害に気づいた後、不当な遅滞なく顧客に通知する。この通知には、少なくとも以下の情報を記載する。 (a) 侵害の性質にかかる詳細(可能であれば、関係するデータ主体とデータ記録のカテゴリーと概数を含む)。 (b) データ侵害に関する詳細情報を入手するための連絡先情報。 (c) データ侵害によって生じる可能性のある影響及び、データ侵害による悪影響を軽減するために実施した、又は実施を提案した措置。 これらの情報の全てを同時に提供することが不可能である場合に限り、最初の通知にはその時点で入手可能な情報を記載し、それ以上の情報は、入手可能になるに従って、後日不当な遅滞なく提供するものとする。また、Staffbaseは、個人データ侵害を抑え、調査し、軽減するために、適切で合理的な措置を講じる。

contain, at least: (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned); (b) the details of a contact point where more information concerning the Personal Data Breach can be obtained; (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay. Staffbase shall also take appropriate and reasonable steps to contain, investigate, and mitigate any Personal Data Breach. The Parties shall set out in Annex III all other elements to be provided by Staffbase when assisting Customer in the compliance with Customer's obligations under Data Protection Laws.	両当事者は、データ保護法に基づく顧客の義務の遵守に関してStaffbaseが顧客を支援する際に提供するその他の全ての要素を、附属書IIIに規定する。
Clause 10 - Non-compliance with the DPA and termination (a) Without prejudice to any provisions of Data Protection Laws, in the event that Staffbase is in breach of its obligations under this DPA, Customer may instruct Staffbase to suspend the processing of Personal Data until the latter complies with this DPA or the contract is terminated. Staffbase shall promptly inform Customer in case it is unable to comply with this DPA, for whatever reason. (b) Customer shall be entitled to terminate the Agreement insofar as it concerns processing of Personal Data in accordance with this DPA if: (1) the processing of Personal Data by Staffbase has been suspended by Customer pursuant to point (a) and if compliance with this DPA is not restored within a reasonable time and in any event within one month following suspension; (2) Staffbase is in substantial or persistent breach of this DPA or its obligations under Data Protection Laws; (3) Staffbase fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this DPA or applicable Data Protection Law. (c) Staffbase shall be entitled to terminate the Agreement insofar as it concerns processing of Personal Data under this DPA where, after having informed Customer that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), Customer insists on compliance with the instructions. (d) Following termination of the contract, Staffbase shall delete all Personal Data processed on behalf of Customer and certify to Customer that it has done so, or, if requested by Customer, return all the Personal Data to Customer and delete existing copies unless Data Protection Law requires storage of the Personal Data. Until the data is deleted or	第**10**条 - **DPA**の不遵守及び解除 (a) データ保護法の規定を損なうことなく、Staffbaseが本DPAに基づく義務に違反した場合、顧客は、Staffbaseに対し、後者が本DPAを遵守するまで、又は契約が解除されるまで、個人データの処理を停止するよう指示することができる。Staffbaseは、理由にかかわらず、本DPAを遵守することができない場合、速やかに顧客に通知する。 (b) 顧客は、以下の場合、本DPAに従った個人データの処理に関する限り、本契約を解除する権利を有する。 (1) Staffbaseによる個人データの処理が、第(a)項に従って顧客により停止され、本DPAの遵守が合理的な期間内に、またいかなる場合も停止から1ヶ月以内に回復されない場合。 (2) Staffbaseが、本DPA又はデータ保護法に基づく自己の義務に、実質的又は持続的に違反する場合。 (3) Staffbaseが、本DPA又はデータ保護法に従った自己の義務に関して、管轄裁判所又は管轄監督機関（複数の場合を含む。）の拘束力ある決定に従わない場合。 (c) Staffbaseが顧客に対し、第7条第1項第(b)号に従って、顧客の指示が適用ある法律上の要件に抵触すると通知したにもかかわらず、顧客がその後も指示に従うよう主張した場合、Staffbaseは、本DPAに基づく個人データの処理に関連する限りにおいて、本契約を解除する権利を有する。 (d) 契約の解除後、Staffbaseは、顧客に代わって処理した全ての個人データを削除し、顧客に対してその実施を証明するか、又は顧客の要請があれば、全ての個人データを顧客に返却し、既存の写しを削除する。但し、データ保護法が個人データの保管を義務づけている場合はその限りではない。Staffbaseは、データを削除し又は返却するまで、本DPAの遵守徹底を継続する。

returned, Staffbase shall continue to ensure compliance with this DPA.	

ANNEX I: **LIST OF PARTIES**	附属書I: 当事者一覧
Customer: **Name:** The Customer as defined in the Order. **Address:** The Customer's address as set out in the Order. **Contact person's name, position and contact details:** The Customer's contact details as set out in the Order or in the Agreement (as applicable). **Signature and accession date:** The Customer's signature and date as set out in the Order.	顧客: 名称:本件注文書の定義に従う顧客。 住所:本件注文書に記載のある顧客の住所。 担当者の氏名、役職及び連絡先:本件注文書又は本契約(いずれか該当する方)に記載のある顧客の連絡先。 署名及び受入日:本件注文書に記載のある顧客の署名及び日付。
Staffbase: **Name:** The Staffbase entity, as defined in the Order. **Address:** Staffbase's address as set out in the Order. **Contact person's name, position and contact details:** privacy@staffbase.com. **Signature and accession date:** Staffbase's signature as set out in the Order or the Agreement.	**Staffbase**: 名称:本件注文書の定義に従うStaffbase法人。 住所: 本件注文書に記載のあるStaffbaseの住所。 担当者の氏名、役職及び連絡先: privacy@staffbase.com。 署名及び受入日:本件注文書に記載のあるStaffbaseの署名。

ANNEX II DESCRIPTION OF THE PROCESSING	附属書II 処理の内容
Categories of data subjects whose Personal Data is processed • Employees or other individuals authorized by Customer to use or get access to the Services; • In relation to the Employee Email and Staffbase Email products, Email Recipients; • In relation to the Communications Control product, Social Media Contacts.	個人データが処理されるデータ主体のカテゴリー • 顧客により本件サービスの使用又はアクセスを許可された従業員又はその他の個人。 • 従業員Eメール及びStaffbase Eメール製品に関連する、Eメールの受信者。 • コミュニケーション管理製品に関連する、ソーシャルメディアの連絡先。

Categories of Personal Data processed	処理される個人データのカテゴリー

Employee App & Front Door Intranet	• **Profile information:** User profile information, such as name, email address, position, department, and location and other required or voluntary profile information • **Login data:** Email address and password. • **Content:** Any other Personal Data contained in Customer Content, for example Personal Data in chats or in media files. • **Technical information:** Device type, IP address, User ID, operation system, browser type, user agent, timestamp of visits and local storage.
Employee Email	• **Account information:** Full name, email address, and password of Authorized Users. • **Email information:** Full name and email address Email Recipients, distribution list names entered into the To and CC fields, content of email newsletter templates and drafts, and subject lines. • **Email metrics information:** Approximate location of Email Recipients (used to identify time zone settings and used in relation to internal email metrics); information about email engagement, including, but not limited to: when an email newsletter is read, when a link in an email newsletter is clicked, collected by tracking technologies such as pixels and cookies; and any optional segmentation information uploaded by Customer, such as the job title, department, or office location. • **Technical information:** Device type, IP address, User ID, operating system, browser type, and visit and usage information.
Staffbase Email	• **Profile information:** User profile information, such as name, email address, position, department, and location and other required or voluntary profile information. • **Login data:** Email address and password of Authorized Users. • **Content:** Any other Personal Data contained in Customer Content, for example Personal Data in email content or in media files. • **Email metrics information:** Information about email engagement, including, but not limited to, when an email newsletter is read, when a link in an email newsletter is clicked, collected by tracking technologies such as pixels and personalized links. • **Technical information:** Device type, IP address, User ID, operation system, browser type, user agent, timestamp of visits and local storage.

Communications Control	• **Account information:** Full name, email address, and password of Authorized Users. • **Social media conversations:** @Handle of social media account, first name and last name of Social Media Contacts, content of message, and conversation history. • **Content:** Any other Personal Data contained in Customer Content. • **Technical information:** Device type, IP address, User ID, operation system, browser type, user agent, timestamp of visits and local storage
従業員アプリ及びフロントドアイントラネット	● プロフィール情報：氏名、Eメールアドレス、役職、所属部署、拠点等のユーザープロフィール情報及び、その他の必須又は任意のプロフィール情報。 ● ログインデータ：Eメールアドレス及びパスワード。 ● コンテンツ：チャットやメディアファイル中の個人データ等、顧客コンテンツに含まれるその他の個人データ。 ● 技術情報：デバイスの種類、IPアドレス、ユーザーID、オペレーションシステム、ブラウザーの種類、ユーザーエージェント、訪問時のタイムスタンプ及びローカルストレージ。
従業員Eメール	● アカウント情報：認定ユーザーの氏名、Eメールアドレス及びパスワード。 ● Eメール情報：Eメール受信者の氏名及びEメールアドレス、To及びCC欄に入力される配信リスト名、Eメールニュースレターテンプレート及び下書きのコンテンツ、並びに件名。 ● Eメールメトリクス情報：Eメール受信者の概略位置（タイムゾーン設定の特定に使用され、また内部Eメールメトリクスに関連して使われる。）、Eメールエンゲージメントに関する情報（いつEメールニュースレターを読んだか、いつEメールニュースレター内のリンクをクリックしたか（ピクセルやクッキー等の追跡技術により収集する。）を含むがそれらに限られない。）、及び、肩書、所属部署、オフィスの所在地等、顧客が任意にアップロードするセグメンテーション情報。 ● 技術情報：デバイスの種類、IPアドレス、ユーザーID、オペレーティングシステム、ブラウザーの種類及び、訪問・使用に関する情報。
Staffbase Eメール	● プロフィール情報：氏名、Eメールアドレス、役職、所属部署、拠点等のユーザープロフィール情報、及び、その他の必須又は任意プロフィール情報。 ● ログインデータ：認定ユーザーのEメールアドレス及びパスワード。 ● コンテンツ：Eメールのコンテンツやメディアファイル中の個人データ等、顧客コンテンツに含まれるその他の個人データ。 ● Eメールメトリクス情報：いつEメールニュースレターを読んだか、いつEメールニュースレター内のリンクをクリックしたか（ピクセルやパーソナライズされたリンク等の追跡技術により収集する。）を含むがそれらに限られない、Eメールエンゲージメントに関する情報。 ● 技術情報：デバイスの種類、IPアドレス、ユーザーID、オペレーションシステム、ブラウザーの種類、ユーザーエージェント、訪問時のタイムスタンプ及びローカルストレージ。
コミュニケーション管理	● アカウント情報：認定ユーザーの氏名、Eメールアドレス及びパスワード。 ● ソーシャルメディアの会話：　ソーシャルメディアアカウントの@ハンドル、ソーシャルメディア連絡先の姓名、メッセージのコンテンツ及び会話履歴。 ● コンテンツ：顧客コンテンツに含まれるその他の個人データ。 ● 技術情報：デバイスの種類、IPアドレス、ユーザーID、オペレーションシステム、ブラウザーの種類、ユーザーエージェント、訪問時のタイムスタンプ及びローカルストレージ

Sensitive data processed (if applicable) and applied	処理されるセンシティブデータ（該当する場合）、及びデータの性質

restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	及びそれに伴うリスクを十分に考慮した適用される制限又は保護手段（例えば厳格な目的の制限、アクセスの制限（専門的なトレーニングを受けたスタッフのみのアクセスを含む）等。）、データへのアクセスの記録の維持、再移転の制限、又は追加のセキュリティ対策。
The extent of any special categories of Personal Data is determined and controlled by Customer and may concern the following categories: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • data concerning health; and • data concerning a natural person's sex life or sexual orientation.	特別なカテゴリーの個人データの範囲は、顧客が決定して、管理するものとし、以下のカテゴリーに関連する場合がある。 • 人種的又は民族的出自 • 政治的見解 • 宗教的又は哲学的信条 • 労働組合の加入状況 • 健康に関するデータ • 自然人の性生活又は性的指向に関するデータ
Nature of the processing Staffbase processes Personal Data to the extent necessary to provide, maintain, support, and improve the Services.	処理の性質 Staffbaseは、本件サービスの提供、維持、サポート及び改善のために必要な範囲内において、個人データを処理する。
Purpose(s) for which the Personal Data is processed on behalf of Customer Staffbase shall process Personal Data as necessary to provide the Services in accordance with the Agreement, as further specified in the Order, and as further instructed by Customer in its use of the Services.	顧客に代わって個人データを処理する目的 Staffbaseは、本契約に従って本件サービスを提供するため、さらに本件注文書に規定された通り、またさらに顧客が本件サービスの利用において指示する通り、必要に応じて個人データを処理する。
Duration of the processing Staffbase shall process Personal Data for the duration of the Subscription Term and for 30 days after at which point the Personal Data is deleted, unless otherwise agreed in writing.	処理期間 Staffbaseは、サブスクリプション期間中及びその後30日間個人データを処理し、この期間の終了時点で個人データを削除する。但し、書面による別段の合意がある場合はその限りではない。
For processing by (sub-) processors, also specify subject matter, nature and duration of the processing Staffbase's Sub-Processors shall process Personal Data as necessary to perform the Services. Subject to Clause 7.7 of the DPA, the Sub-Processors shall process Personal Data during the Subscription Term and for 30 days after at which point the Personal Data is deleted, unless otherwise agreed in writing.	（復）処理者による処理については、処理の主題、性質及び期間も規定する Staffbaseの復処理者は、本件サービスを履行するため必要に応じて個人データを処理する。本DPA第7条第7項を条件として、復処理者は、サブスクリプション期間中及びその後30日間個人データを処理し、この期間の終了時点で個人データを削除する。但し、書面による別段の合意がある場合はその限りではない。

ANNEX III SECURITY MEASURES	附属書III セキュリティ対策
1 SECURITY CERTIFICATIONS ***ISO 27001***: Staffbase's information security management system (ISMS) is ISO/IEC 27001:2013 certified. Customer may download a copy of Staffbase's most recent ISO certificates at https://staffbase.com/en/security/. **System and Organization Controls (SOC) 2 Report ("SOC 2")**: Staffbase's ISMS is SOC 2 certified. Subject to confidentiality agreements being in place, Staffbase will make a copy of the then current SOC 2 Type 2 report, or report or other documentation describing the controls implemented by Staffbase that replace or are substantially equivalent to the SOC 2 report, to Customer on request. ***Communications Control Specific - Security:*** Customer agrees and acknowledges that the SOC 2 certification is not (yet) applicable to the Staffbase Service 'Communications Control'.	**1 セキュリティ認証** ***ISO 27001***：Staffbaseの情報セキュリティマネジメントシステム（ISMS）は、ISO/IEC 27001:2013認証を取得している。顧客は、https://staffbase.com/en/security/からStaffbaseの最新のISO認証書をダウンロードすることができる。 **SOC（System and Organization Controls）2** レポート（以下「**SOC 2**」という。）：StaffbaseのISMSは、SOC 2認証を取得している。秘密保持契約が締結されていることを条件として、Staffbaseは、その時点で有効なSOC 2タイプ2レポートの写し、又はSOC 2レポートに代替するか、実質的に同等の、Staffbaseが施行した管理手段を説明するレポート若しくはその他のドキュメントを、要請に応じて顧客に提供する。 コミュニケーション管理に特化したもの - セキュリティ：顧客は、SOC 2認証がStaffbaseの本件サービス「コミュニケーション管理」には（まだ）適用されないことに同意し、それを認める。
2 ACCESS CONTROLS ***Physical Access Control:*** Staffbase takes reasonable measures to prevent unauthorized persons from gaining physical access to Customer Content. Security measures include but may not be limited to: **(a)** The applications are hosted in ISO 27001 certified data centers. Physical access to these data centers is highly restricted. **(b)** Access to the Staffbase offices is limited to Staffbase employees and authorized individuals. Guests are welcomed at the door and accompanied to the contact person. The issue and return of the access media is documented in writing. **(c)** Access to the Staffbase offices is timely removed in the event of a change in job responsibilities or job status. ***Employee App / Front Door Intranet / Staffbase Email Specific: Internal Access Control:*** Staffbase takes reasonable measures to prevent unauthorized Staffbase personnel from gaining access to Customer Content. Security measures include but may not be limited to: **(a)** A selected number of Staffbase personnel has access to Personal Data in the following roles: **3rd Level Access – System administrator:** Personal access to all Personal Data within the corresponding customer instance, including the database. **2nd Level Access – Support Administration:** Personalized access to all Personal Data within the associated customer instance, but no server or database access. **1st Level Access – Customer Success Access:** Access to all Personal Data within a customer instance through the application according to Customer's approval. No access to databases is available. Customer Support Access is not person-specific and is available to all members of Staffbase's customer success and customer support teams. **(b)** The roles defined above are assigned to the minimum number of Staffbase personnel. The allocation of roles is recorded and reviewed at least once a year.	**2 アクセス管理** 物理的アクセス管理：Staffbaseは、許可なき者が顧客コンテンツに物理的にアクセスすることを防止するため、合理的な措置を講じる。セキュリティ対策には、以下が含まれるがこれらに限られない。 **(a)** アプリケーションは、ISO 27001認証を取得したデータセンターでホストされる。これらのデータセンターへの物理的なアクセスは、厳しく制限されている。 **(b)** Staffbaseのオフィスへのアクセスは、Staffbaseの従業員及び許可された者に限定される。訪問客は入り口で迎えられ、担当者のもとまで同行される。アクセスメディアの発行及び返却は、書面で記録される。 **(c)** 職責又は業務状況の変更があった場合、Staffbaseのオフィスへのアクセスは、適時に終了する。 従業員アプリ／フロントドアイントラネット／***Staffbase E***メールに特化したもの：内部アクセス管理：Staffbaseは、許可を受けていないStaffbase人員が顧客コンテンツにアクセスすることを防止するため、合理的な措置を講じる。セキュリティ対策には、以下が含まれるがこれらに限られない。 **(a)** Staffbase人員の一部の者が、以下の役割で個人データにアクセスできる。 レベル**3**アクセス – システム管理者：データベースを含め、対応するカスタマーインスタンス内の全ての個人データへの個人的なアクセス。 レベル**2**アクセス – サポート業務：関連するカスタマーインスタンス内の全ての個人データへの、パーソナライズされたアクセス。サーバー又はデータベースにはアクセスできない。 レベル**1**アクセス – カスタマーサクセスのアクセス：顧客の承認に従った、カスタマーインスタンス内の全ての個人データへのアプリケーション経由のアクセス。データベースにはアクセスできない。カスタマーサポートアクセスは特定個人に依存せず、Staffbaseのカスタマーサクセス及びカスタマーサポートチームのメンバー全員がアクセスできる。 **(b)** 上記に定義する役割は、最低限のStaffbase人員に与えられる。役割の配分は記録され、少なくとも1年に1回見直す。 従業員***E***メールに特化したもの：内部アクセス管理：顧客が従業員Eメールを購入した場合、Staffbaseは、許可を受けていないStaffbase人員が従業員Eメールに関連して処理される個人データにアクセスすることを防止するため、合理的な措置を講じる。従業員Eメールに関連するセキュリティ対策には、以下が含まれるがこれらに限られない。 **(a)** Staffbase人員のうち一部の者が、以下の役割で個人データにアクセスできる。

Employee Email Specific: Internal Access Control. If Customer has purchased Employee Email, then Staffbase will take reasonable measures to prevent unauthorized Staffbase personnel from gaining access to Personal Data processed in relation to Employee Email. Security measures related to Employee Email include but may not be limited to: **(a)** A selected number of Staffbase personnel has access to Personal Data in the following roles: **Developer Access:** Personal access to all Personal Data within the corresponding customer instance, including the database. **Customer Success Access:** Personal access to the customer instance on behalf of the respective Admin User, but no server or database access. **(b)** The roles defined above are assigned to the minimum number of Staffbase personnel. The allocation of roles is recorded and reviewed at least once a year. ***Communications Control Specific: Internal Access Control:*** If Customer has purchased Communications Control, then Staffbase will take reasonable measures to prevent unauthorized Staffbase personnel from gaining access to Personal Data processed in relation to Communications Control. Security measures related to Communications Control include but may not be limited to: **(a)** A selected number of Staffbase personnel has access to Personal Data in the following roles: **3rd Level Access – System administrator:** Personal access to all Personal Data within the corresponding customer instance, including the database. **2nd Level Access – Support Administration:** Personalized access to all Personal Data within the associated customer instance, and limited access to server or database access. **1st Level Access – Customer Success Access:** Access to all Personal Data within a customer instance through the application according to Customer's approval. No access to databases is available. Customer Support Access is not person-specific and is available to all members of Staffbase's customer success and customer support teams. **(b)** The roles defined above are assigned to the minimum number of Staffbase personnel. The allocation of roles is recorded and reviewed at least once a year.	デベロッパーアクセス：データベースを含め、対応するカスタマーインスタンス内の全ての個人データへの個人的なアクセス。 カスタマーサクセスのアクセス：対応する管理ユーザーに代わる、カスタマーインスタンスへの個人的なアクセス。サーバー又はデータベースにはアクセスできない。 **(b)** 上記に定義する役割は、最低限のStaffbase人員に与えられる。役割の配分は記録され、少なくとも1年に1回見直す。 コミュニケーション管理に特化したもの ：内部アクセス管理：顧客がコミュニケーション管理を購入した場合、Staffbaseは、許可を受けていないStaffbase人員がコミュニケーション管理に関連して処理される個人データにアクセスすることを防止するため、合理的な措置を講じる。コミュニケーション管理に関連するセキュリティ対策には、以下が含まれるがこれらに限られない。 **(a)** Staffbase人員のうち一部の者が、以下の役割で個人データにアクセスできる。 レベル**3**アクセス – システム管理者：データベースを含め、対応するカスタマーインスタンス内の全ての個人データへの個人的なアクセス。 レベル**2**アクセス – サポート業務：関連するカスタマーインスタンス内の全ての個人データへのパーソナライズされたアクセス、及び、サーバー又はデータベースへの制限されたアクセス。 レベル**1**アクセス – カスタマーサクセスのアクセス：顧客の承認に従った、カスタマーインスタンス内の全ての個人データへのアプリケーション経由のアクセス。データベースにはアクセスできない。カスタマーサポートアクセスは特定個人に依存せず、Staffbaseのカスタマーサクセス及びカスタマーサポートチームのメンバー全員がアクセスできる。 **(b)** 上記に定義する役割は、最低限のStaffbase人員に与えられる。役割の配分は記録され、少なくとも1年に1回見直す。
3 ELECTRONIC ACCESS CONTROLS Staffbase will take reasonable measures to prevent unauthorized persons from gaining electronic access to Customer Content. Security measures include but may not be limited to: **(a)** Access to the data processing system is limited to authorized individuals and requires identification and successful authentication by username and password using state-of-the-art security measures. **(b)** Authentication media and access codes to access	**3** 電子的アクセス管理 Staffbaseは、許可なき者が顧客コンテンツに電子的にアクセスすることを防止するため、合理的な措置を講じる。 セキュリティ対策には、以下が含まれるがこれらに限られない。 **(a)** データ処理システムへのアクセスは、許可された者に限定され、最新のセキュリティ対策を使った本人確認及びユーザー名とパスワードによる認証の成功を必要とする。 **(b)** レベル3又はレベル2でデータ処理システムにアクセスするための認証メディア及びアクセスコードは、個人認証情報（パスワードとユーザーID）にリンクされている。一時的に雇

data processing systems on 3rd and 2nd Level are linked to personal credentials (password and user ID). Authentication codes for temporarily employed persons (external developers, interns, trainees) are allocated individually. No reusable IDs (e. g. trainee1, etc.) are assigned. **(c)** A process for requesting, approving, issuing and withdrawing authentication media and access authorizations has been set up and documented. **(d)** All workstations and terminals are protected against unauthorized access through both automatic and manual password-protected locking so they are locked within 5 minutes latest. Internal training is provided to support the regular use of both mechanisms. **(f)** Passwords are managed by password managers. Access to the workstations and password manager is password protected.	用されている者（外部デベロッパー、インターン、研修生）の認証コードは、個別に配分される。再使用可能なID（例えばtrainee1等）は付与されない。 **(c)** 認証メディア及びアクセス許可の要求、承認、発行及び撤回の手続は、規定され文書化されている。 **(d)** 全てのワークステーション及びターミナルは、自動・手動の両方のパスワード保護付きロックにより、不正アクセスに対して保護されており、遅くとも5分以内にロックされる。両方のメカニズムについて、定期的な使用をサポートするため、内部トレーニングが提供されている。 **(f)** パスワードは、パスワードマネージャーにより管理されている。ワークステーション及びパスワードマネージャーへのアクセスは、パスワード保護されている。
4 ISOLATION CONTROLS. Staffbases' testing and staging systems are separated logically from production systems. For testing, Staffbase facilitates dedicated test data.	**4 隔離管理** Staffbaseの試験及びステージングシステムは、論理的に生産システムから分かれている。試験のため、Staffbaseは、専用のテストデータを用意する。
5 PSEUDONYMIZATION AND ENCRYPTION **Encryption.** All communication of our systems over public networks is encrypted according to the state of the art. Staffbase encrypts user passwords by using best-practice one-way hash functions and the core databases are encrypted at rest using industry best practices encryption schemes. **Pseudonymization.** Staffbase uses pseudonyms for storing user related interactions whenever possible.	**5 仮名化及び暗号化** 暗号化。当社システムの公共ネットワーク上における全てのコミュニケーションは、最新の方法に従って暗号化されている。Staffbaseは、ベストプラクティスの一方向ハッシュ関数を使ってユーザーのパスワードを暗号化し、コアデータベースは、業界ベストプラクティスの暗号化方式を使用して、保存データの暗号化が行われている。 仮名化。Staffbaseは、ユーザー関連のインタラクションを、できる限り仮名を使用して保管する。
6 INTEGRITY **Data Transfer Control:** Data is transferred exclusively using the encrypted HTTPS protocol. **Data Entry Control:** Customer's activities related to the creation and update of user data records are logged.	**6 完全性** データ移転管理：データは、専ら暗号化HTTPSプロトコルを使用して移転される。 データ入力管理：ユーザーデータ記録の生成及び更新に関連する顧客の活動は、ログ記録される。
7 AVAILABILITY AND RESILIENCE Staffbase has designed a system meant to minimize any service disruptions resulting from natural disasters, hardware failure, or other unforeseen disasters or catastrophes. Staffbase's Disaster Recovery approach includes: **(a)** Using state-of-the-art service providers to help deliver the Services; **(b)** Backups. Staffbase performs daily backups on all relevant systems, which are stored for up to a month and available for restoration based on identified incidents; **(c)** Dual mode. All production systems run at least in dual-mode to provide a fast performing failover; **(d)** Global offices. Staffbase operates worldwide, and in the event of regional issues in one of Staffbase's offices, our teams in other locations can support to help recover smoothly; and **(e)** Disaster Recovery Planning. Staffbase's disaster recovery program focuses on technical disasters for operation of the Staffbase platform and includes	**7 可用性及びレジリエンス** Staffbaseは、自然災害、ハードウェア障害又はその他の予期しない災害又は惨事に起因するサービス障害を最小限に抑えることを意図したシステムを設計した。Staffbaseの災害復旧のアプローチには、以下が含まれる。 **(a)** 本件サービスの提供を支援するため、最先端のサービスプロバイダーを使用 **(b)** バックアップ。Staffbaseは、全ての関連システムについて毎日バックアップを実施し、バックアップは最長1ヶ月間保管され、特定されたインシデントに基づき回復できるよう利用可能である。 **(c)** デュアルモード。全ての生産システムは少なくともデュアルモードで動作し、高速のフェイルオーバーを提供する。 **(d)** グローバルオフィス。Staffbaseは世界中で事業展開しており、Staffbaseのオフィスのひとつで地域的な問題が生じた場合、他の拠点のチームがサポートして、スムーズな復旧を支援することができる。 **(e)** 災害復旧計画。Staffbaseの災害復旧プログラムは、Staffbaseプラットフォームの運用のための技術的災害に焦点を当てており、復旧チームの定期的トレーニングと共に、異なるシナリオでの計画も含む。そのため、チームは非

plans for different scenarios as well as regular training for the recovery team. The team is therefore able to regain data in cases of emergency.	常事態でもデータを回復することができる。
8 TESTING, ASSESSMENT, AND EVALUATION ***Data Protection Management:*** Staffbase has defined processes and workflows for the processing of Personal Data. Implementation is regularly monitored by the security and legal team. ***Training:*** All employees of Staffbase receive annual security and data protection awareness training. ***Customer instructions:*** The persons authorized on the part of Staffbase to accept and execute instructions from Customer are specified by Staffbase in a binding manner. In general, these are the Customer's account manager and staff members of the Staffbase customer success and support team.	**8 試験、評価及び査定** データ保護管理：Staffbaseは、個人データの処理に関するプロセス及びワークフローを定義している。実施状況は、セキュリティ及び法務チームが定期的に監視する。 トレーニング：Staffbaseの従業員は全員、毎年セキュリティ・データ保護意識向上トレーニングを受ける。 顧客の指示：Staffbaseにおいて顧客からの指示を受け入れ、実行する権限のある者は、Staffbaseにより拘束力のある形で指定されている。一般的に、これらは顧客のアカウントマネージャー、並びに、Staffbaseのカスタマーサクセス及びサポートチームのメンバーである。
9 SECURITY INCIDENT MANAGEMENT All employees, contractors, and key suppliers are required to report security incidents. Staffbase has a plan to promptly and systematically respond to any security or availability incidents that may happen. The Staffbase Incident Response Plan is based on industry standards and consists of four stages designed to help prevent, identify, and remediate security incidents. Our Incident Response Plan also includes a Problem Management process, designed to identify root causes and correct unknown security incidents. The entire security team is trained to respond according to the established Incident Response Plan. Personal Data Breach procedures are included on the Incident Response Plan and for those incidents, the involvement of the Data Protection and Legal team is required. Affected customers are notified of Personal Data Breaches in accordance with the DPA. This plan is reviewed and updated on a regular basis as part of Staffbase's ISO 27001 certification.	**9 セキュリティインシデント管理** 全ての従業員、請負者及び主要サプライヤーは、セキュリティインシデントを報告する義務を負う。Staffbaseは、発生するセキュリティ又は可用性インシデントに対して速やかにかつ系統的に対応する計画がある。Staffbaseインシデント対応計画は、業界標準に基づいており、セキュリティインシデントの予防、特定、是正に役立つ4段階のステージで構成されている。 また、インシデント対応計画には、問題管理プロセスが含まれており、未知のセキュリティインシデントの根本原因を特定し、是正するよう設計されている。セキュリティチーム全体が、確立されたインシデント対応計画に従って対応するようトレーニングを受けている。インシデント対応計画には個人データ侵害対応手続が含まれており、このようなインシデントでは、データ保護及び法務チームの関与が義務づけられる。個人データ侵害の影響を受けた顧客は、DPAに従って通知を受ける。 本計画は、StaffbaseのISO 27001認証の一環として定期的に見直され、更新される。
10 VULNERABILITY MANAGEMENT A vulnerability management process is established for the Staffbase products, to ensure that vulnerabilities are identified, evaluated, and resolved in a timely manner. Staffbase uses the industry standard CVSS score to evaluate the severity of identified vulnerabilities. Staffbase contracts with a third party penetration tester to perform independent penetration tests at least annually. A summary for the most recent penetration test is available on request under a Non-Disclosure Agreement. Internal penetration tests are also performed on a regular basis to be compliant with SOC 2 requirements. Staffbase has launched a private bug bounty program for continuous security testing by a global community of ethical hackers. The bug bounty program has helped improve our security controls for the Employee App and Front Door Intranet product with great success. There is a plan to extend the bug bounty program to our other products as well.	**10 脆弱性管理** 脆弱性が特定され、評価され、適時に解決されるよう徹底するため、Staffbase製品に関して脆弱性管理プロセスが確立されている。Staffbaseは、業界標準のCVSSスコアを使用して、特定された脆弱性の深刻度を評価する。 Staffbaseは、第三者ペネトレーションテスターに委託して、少なくとも年1回独立ペネトレーションテストを実施する。最新のペネトレーションテストの概要は、要請があれば秘密保持契約に基づいて閲覧可能である。また、SOC 2の要件に準拠するため、内部ペネトレーションテストも定期的に実施される。 Staffbaseは私設のバグバウンティプログラムを設立し、世界のエシカルハッカーコミュニティによる継続的なセキュリティテストを実施している。バグバウンティプログラムは、従業員アプリ及びフロントドアイントラネット製品のセキュリティ管理向上で、多大な成功を収めた。バグバウンティプログラムを、他の製品にも拡張する計画がある。

ANNEX IV **LIST OF SUB-PROCESSORS**	**附属書IV** 復処理者リスト
An up-to-date overview of Staffbase Sub-Processors can be found at: https://staffbase.com/en/legal/subprocessors/	最新のStaffbase復処理者の概要は、 https://staffbase.com/en/legal/subprocessors/に掲載されている。

ANNEX V MODEL CLAUSES FOR RESTRICTED TRANSFERS UNDER EUROPEAN DATA PROTECTION LAW	附属書V 欧州データ保護法に基づく制限対象移転に関するモデル条項
1 Applicability of the Model Clauses, Modules 2 & 3 **(a) European Union (GDPR).** The parties agree that when the transfer of Personal Data from Customer (as "data exporter") to Staffbase (as "data importer") is a Restricted Transfer and the GDPR requires that appropriate safeguards are put in place, the transfer shall be subject to the Model Clauses, which are deemed incorporated into and form a part of this DPA by reference, as follows: **(i)** Module 2 (Controller-to-Processor) shall apply where Customer is a data controller and Staffbase is a data processor of Personal Data; Module 3 (Processor-to-Processor) shall apply where both Customer and Staffbase are data processors of Personal Data. For each Module, where applicable: **(ii)** in Clause 7, the optional docking clause does not apply; **(iii)** in Clause 8.9, any audits by Customer shall be carried out in accordance with Clause 7.6 of this DPA; **(iv)** in Clause 9, Option 2 shall apply. For clarity, Staffbase has Customer's general authorization to engage Sub-Processors in accordance with Clause 7.7 of this DPA; **(v)** in Clause 11(a), the optional language shall not apply; **(vi)** in relation to Clause 12, any claims brought under the Model Clauses shall be subject to the terms and conditions set forth in the Agreement. For clarity, in no event shall any party limit its liability towards data subjects under the Model Clauses; **(vii)** in Clause 17, Option 1 shall apply. The parties agree that the governing law for disputes related to the Model Clauses shall be determined in accordance with the 'Governing Law' section of the Agreement or, if such section does not specify an EU Member State, the Model Clauses shall be governed by the laws of Ireland; **(viii)** in Clause 18(b), the parties agree that the forum for disputes related to the Model Clauses shall be determined in accordance with the 'Jurisdiction and Venue' section of the Agreement or, if such section does not specify an EU Member State, disputes shall be resolved before the courts of Dublin, Ireland; **(ix)** Annex I of the Model Clauses, shall be deemed completed with the information set out in Annex 1 and Annex 2 of this DPA; and **(x)** Annex II of the Model Clauses, shall be deemed completed with the information set out in Annex III of this DPA. **(b) UK (UK Data Protection Law).** The parties agree that when the transfer of Personal Data from Customer (as	**1** モデル条項モジュール**2**及び**3**の適用可能性 **(a)** 欧州連合(**GDPR**)。両当事者は、(「データ輸出者」としての)顧客から(「データ輸入者」としての)Staffbaseへの個人データの移転が制限対象移転であり、GDPRにより適切な保護手段の実施が義務づけられる場合、当該の移転はモデル条項の対象となり、モデル条項は以下の通り参照することにより本DPAに組み入れられ、その不可分の一部をなすとみなされることに合意する。 **(i)** モジュール2(管理者から処理者への移転)は、顧客が個人データのデータ管理者、Staffbaseがデータ処理者である場合に適用され、モジュール3(処理者から処理者への移転)は、顧客とStaffbaseの両方が個人データのデータ処理者である場合に適用される。各モジュールについて、該当する場合、以下のとおりとする。 **(ii)** 第7条において、オプションのドッキング条項は適用されない。 **(iii)** 第8条第9項において、顧客による監査は、本DPA第7条第6項に従って実施される。 **(iv)** 第9条において、オプション2が適用される。明確にするために付言すると、Staffbaseは顧客から、本DPA第7条第7項に従って、復処理者を起用する一般的許可を得ている。 **(v)** 第11条第(a)号において、オプション言語は適用されない。 **(vi)** 第12条に関連して、モデル条項に基づいて申し立てられた請求には、本契約に定める条件が適用される。明確にするために付言すると、いかなる場合においても、いずれの当事者も、データ主体に対するモデル条項に基づく責任を限定しない。 **(vii)** 第17条において、オプション1が適用される。両当事者は、モデル条項に関連する紛争の準拠法が本契約の「準拠法」条項に従って決定され、又は、当該条項がEU加盟国を特定しない場合、モデル条項がアイルランド法に準拠することに合意する。 **(viii)** 第18条第(b)号において、両当事者は、モデル条項に関連する紛争解決の場が本契約の「管轄権と裁判地」条項に従って決定され、又は、当該条項がEU加盟国を特定しない場合、紛争がアイルランドのダブリンの裁判所で解決されることに合意する。 **(ix)** モデル条項附属書Iは、本DPA附属書1及び附属書2に記載のある情報をもって完成したものとみなされる。 **(x)** モデル条項附属書IIは、本DPA附属書IIIに記載のある情報をもって完成したものとみなされる。 **(b)** 英国(英国データ保護法)。両当事者は、(「データ輸出者」としての)顧客から(「データ輸入者」としての)Staffbaseへの個人データの移転が、英国データ保護法に基づく制限対象移転である場合、本DPA第7条第8項第(c)号に基づいて組み入れられるモデル条項が、以下の変更を加えて適用されることに合意する。 **(i)** モデル条項は、英国補遺に規定する通り変更され、参照することにより組み入れられ、本DPAの不可分の一部となる。 **(ii)** 英国補遺第1部の表1、2及び3は、本DPA附属書II、附属書III及び附属書IVに記載のある情報をもって完成したものとみなされる。 **(iii)** 英国補遺第1部の表4は、「いずれの当事者も不該当」を選択することにより完成したものとみなされる。 **(iv)** モデル条項と英国補遺の間に矛盾がある場合、英国補遺第10条及び第11条に従って解決するものとする。 **(c)** スイス(**FADP**)。両当事者は、(「データ輸出者」としての)顧客から(「データ輸入者」としての)Staffbaseへの個人データの移転が、FADPに基づく制限対象移転である場合、本DPA第7条第8

"data exporter") to Staffbase (as "data importer") is a Restricted Transfer under UK Data Protection Law, the Model Clauses as incorporated under Clause 7.8(c) if this DPA shall apply with the following modifications: **(i)** the Model Clauses shall be amended as specified by the UK Addendum, which shall be incorporated by reference and form an integral part of this DPA; **(ii)** Tables 1, 2, and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex II, Annex III, and Annex IV of this DPA; **(iii)** Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party"; and **(iv)** any conflict between the Model Clauses and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. **(c) Switzerland (FADP).** The parties agree that when the transfer of Personal Data from Customer (as "data exporter") to Staffbase (as "data importer") is a Restricted Transfer under the FADP, the Model Clauses as incorporated under Clause 7.8(c) of this DPA shall apply with the following modifications: **(i)** in Clause 13, the competent supervisory authority is the FDPIC; **(ii)** references to "EU", "Union", and "Member State" in the Model Clauses refer to Switzerland; **(iii)** the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of accessing their rights; and **(iv)** references to the "General Data Protection Regulation," "Regulation 2016/679," and "GDPR" in the Model Clauses refer to the FADP.	項第(c)号に基づき組み入れられるモデル条項が、以下の変更を加えて適用されることに合意する。 **(i)** 第13条において、管轄監督機関はFDPICである。 **(ii)** モデル条項における「EU」、「連合」及び「加盟国」への言及は、スイスへの言及とする。 **(iii)** 「加盟国」という用語を、スイスのデータ主体が自らの権利にアクセスする可能性を除外するような形で解釈してはならない。 **(iv)** モデル条項における「一般データ保護規則」、「規則2016/679」及び「GDPR」への言及は、FADPへの言及とする。

2 Processing Details under Annex I of the Model Clauses	**2** モデル条項附属書Iに基づく処理の詳細
A List of Parties	**A** 当事者一覧

Data Exporter	**Data Importer**
Name: The Customer, as defined in the Order	**Name:** The Staffbase entity as defined in the Order
Address: Customer's address, as set out in the Order	**Address:** Staffbase's address, as set out in the Order
Contact person's name, position and contact details: The Customer's contact details, as set out in the Order	**Contact person's name, position and contact details:** privacy@staffbase.com
Role: Controller	**Role:** Processor
Activities relevant to the data transferred under the Model Clauses: Processing of Personal Data in connection with Customer's use of the Services	
データ輸出者	データ輸入者

名称:本件注文書の定義に従う顧客	名称:本件注文書の定義に従うStaffbase法人
住所:本件注文書に記載のある顧客の住所	住所:本件注文書に記載のあるStaffbaseの住所
担当者の氏名、役職及び連絡先: 本件注文書に記載のある顧客の連絡先	担当者の氏名、役職及び連絡先: privacy@staffbase.com
役割:管理者	役割:処理者
モデル条項に基づいて移転されるデータに関連する活動 顧客による本件サービスの利用に関連する個人データの処理	

B Description of Transfer	B 移転の概要
Categories of Data Subjects	See Annex II of this DPA
Categories of Personal Data	See Annex II of this DPA
Sensitive data (if applicable)	See Annex II of this DPA
Frequency of the transfer	Continuous basis depending on the use of the Services by Customer.
Nature of the processing	See Annex II of this DPA
Purpose(s) of the transfer	See Annex II of this DPA
Duration of the processing	Staffbase shall process Personal Data for the duration of the Subscription Term and for 30 days after, at which point the Personal Data is deleted, unless otherwise agreed upon in writing.
Sub-Processor transfers	Staffbase's Sub-Processors shall process Personal Data as necessary to perform the Services. Subject to Clause 7.7 of the DPA, the Sub-Processors shall process Personal Data for the duration of the Subscription Term and for 30 days after, at which point the Personal Data is deleted, unless otherwise agreed in writing.
データ主体のカテゴリー	本DPA附属書IIを参照
個人データのカテゴリー	本DPA附属書IIを参照
センシティブデータ（該当する場合）	本DPA附属書IIを参照
移転の頻度	顧客による本件サービスの利用状況により、継続的に実施
処理の性質	本DPA附属書IIを参照
移転の目的	本DPA附属書IIを参照
処理期間	Staffbaseは、サブスクリプション期間中及びその後30日間個人データを処理し、この期間の終了時点で個人データを削除する。但し、書面による別段の合意がある場合はその限りではない。
復処理者による移転	Staffbaseの復処理者は、本件サービスを履行するため必要に応じて個人データを処理する。本DPA第7条第7項を条件として、復処理者は、サブスクリプション期間中及びその後30日間個人データを処理し、この期間の終了時点で個人データを削除する。但し、書面による別段の合意がある場合はその限りではない。

C Competent Supervisory Authority	C 管轄監督機関
For the purposes of the Model Clauses, the supervisory authority that shall act as competent supervisory authority is either: **(i)** where Customer is established in an EU Member State, the supervisory authority responsible for ensuring Customer's compliance with the GDPR; **(ii)** where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU Member State in which Customer's representative is established; or **(iii)** where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the supervisory authority of the EU Member State in which the Data Subjects are predominantly located. In relation to Personal Data that is subject to UK Data Protection Law, the competent supervisory authority is the UK Information Commissioner's Office. In relation to Personal Data that is subject to the FADP, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner (as applicable).	モデル条項の目的において、管轄監督機関として行動する監督機関は、以下のいずれかであるものとする。(i)顧客がEU加盟国内に設立されている場合、顧客のGDPR準拠徹底に対して責任を有する監督機関。(ii)顧客がEU加盟国内に設立されていないが、GDPRの域外適用範囲に該当し、代表者を任命している場合、顧客の代表者の設立拠点であるEU加盟国の監督機関。(iii)顧客がEU加盟国内に設立されていないが、GDPRの域外適用範囲に該当し、代表者を任命していない場合、データ主体が主に所在するEU加盟国の監督機関。英国データ保護法の対象となる個人データに関しては、英国情報コミッショナーオフィスを管轄監督機関とする。FADPの対象となる個人データに関しては、スイス連邦データ保護情報コミッショナーを管轄監督機関とする（該当する場合）。