Staffbase Data Processing Agreement

1 INTRODUCTION

(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.

(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.

(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.

(d) The DPA shall prevail if there is a conflict between the Agreement and the DPA.

(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.

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 Laws, **(ii)** US State Privacy Laws, **(iii)** Canadian Privacy Laws, and **(iv)** Australian Privacy Laws.

"**European Data Protection Laws**" 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 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 Laws apply, 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 Laws apply, 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 State 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: https://staffbase.com/en/legal/. To the extent that Staffbase processes Personal Data governed by US State 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.

Clause 2 – Invariability of the Clauses [Not applicable]

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.

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.

Clause 5 - Docking clause [Not applicable]

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.

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 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 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

(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.

(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.

(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.

(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.

(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 Laws 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 Laws require 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;

(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 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.

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

ANNEX I:

LIST OF PARTIES

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.

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.

ANNEX II

DESCRIPTION OF THE PROCESSING

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.

Categories of Personal Data processed

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

Sensitive data processed (if applicable) and applied 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.

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.

Nature of the processing

Staffbase processes Personal Data to the extent necessary to provide, maintain, support, and improve the Services.

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.

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.

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.

ANNEX III

SECURITY MEASURES

1 SECURITY CERTIFICATIONS

ISO 27001: Staffbase's information security management system (ISMS) is ISO/IEC 27001:2022 certified. Customers may download a copy of Staffbase's most recent ISO certificates directly from the Trust Center (trust.staffbase.com).

System and Organization Controls (SOC) 2 Report ("SOC 2"): Staffbase's ISMS is SOC 2 certified. Subject to confidentiality agreements being in place, the current SOC 2 Type 2 report may be downloaded directly from the Trust Center (trust.staffbase.com).

Additional security certifications and compliance documentation can be found in our Trust Center.

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 and underlies stringent requirements from our hosting providers.

(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 are documented in writing.

(c) Access to the Staffbase offices is timely removed or modified in the event of a change in job responsibilities or job status.

Access to Customer Data: 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 have access to Personal Data in the following roles:

3rd Level Access – System administrator: Personal access to all Personal Data and all customer content within the corresponding customer instance, including the database.

2nd Level Access – Support Administration: Personalized access to all Personal Data and customer data within the associated customer instance, but no server or database access.

1st Level Access – Customer Success Access: Access to all Personal Data and customer 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 following Role Based Access Control and Least-Privilege models. The allocation of roles is recorded and reviewed at least once a year.

3 ELECTRONIC ACCESS CONTROLS

Staffbase will take reasonable measures to prevent unauthorized persons from gaining electronic access to Personal Data. Security measures include but may not be limited to:

(a) Access to the data processing system is limited to authorized individuals and requires successful identification and multi-factor authentication using state-of-the-art security measures.

(b) Authentication media and access codes to access 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.

(e) Passwords are managed by password managers. Access to the workstations and password manager is password protected. Password requirements comply with the ISO 27001.

(f) Accounts are uniquely and identifiably attributed. The use of shared accounts is prohibited and underlies strict approval, documentation, verification and stringent review processes.

4 ISOLATION CONTROLS

Staffbases' development and staging systems are separated logically from production systems. For testing, Staffbase facilitates dedicated test data that does not contain customer data.

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 practice encryption schemes.

Pseudonymization. Staffbase uses pseudonyms for storing user-related interactions whenever possible.

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.

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) Service quality: Staffbase uses 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.

(e) Disaster Recovery Planning: Staffbase's disaster recovery program focuses on technical disasters for the operation of the Staffbase platform and includes 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.

8 TESTING, ASSESSMENT, AND EVALUATION

Data Protection Management: Staffbase has defined processes and workflows for the processing of any Personal and Customer 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.

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 several 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. Data Breach procedures are included in 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.

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, to be compliant with SOC 2 requirements. A summary of the most recent penetration test is available in the Trust Center (trust.staffbase.com).

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 our Employee App & Front Door Intranet product with great success.

ANNEX IV

LIST OF SUB-PROCESSORS

An up-to-date overview of Staffbase Sub-Processors can be found at: https://staffbase.com/en/legal/subprocessors/.

ANNEX V

MODEL CLAUSES FOR RESTRICTED TRANSFERS UNDER EUROPEAN DATA PROTECTION LAWS

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 "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.

2 Processing Details under Annex I of the Model Clauses

A List of Parties

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	

B Description of Transfer

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.

C Competent Supervisory Authority

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).