Please see staffbase.com for the latest version of this information.

Staffbase Data Processing Agreement

This is an archived version of the Staffbase Data Processing Agreement. View the current version (URL: https://staffbase.com/en/legal/dpa/) or all past versions (URL: https://staffbase.com/en/legal/dpa/archive/).

17 August 2021

This Staffbase Data Processing Agreement (**"DPA"**) forms part of the Staffbase Terms of Service (URL: https://staffbase.com/en/terms/), or, if applicable, the signed Master Subscription Agreement between Staffbase and the Customer (in either case, the **"Governing Agreement"**). In the event of any conflict between the "Governing Agreement" and the DPA, the DPA will prevail.

1 DEFINITIONS.

1.1 **"Affiliate"** has the same meaning as in the Governing Agreement.

1.2 **"Applicable Privacy Law"** means all applicable laws and regulations relating to data protection and privacy the Customer is subject to and which apply to the processing of Personal Data under the Governing Agreement. Applicable Privacy Law includes, where applicable: (i) EU Data Protection Law; (ii) the CCPA; (iii) in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data protection and privacy as a consequence of the United Kingdom leaving the European Union; and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case as amended, repealed, superseded or replaced from time to time.

1.3 **"CCPA"** means the California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018), and its implementing regulations,

Cal. Code Regs. tit. 11, § 999.300 et seq. To the extent Staffbase processes any Personal Data protected by the CCPA, the terms in **Exhibit 3 ("CCPA Specific Terms")** apply in addition to the terms of this DPA.

1.4 **"EU Data Protection Law"** means all data protection laws and regulations applicable to the European Union (**"EU"**), the European Economic Area (**"EEA"**) and their member states, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (**"GDPR"**); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; as amended by the Directive 2009/136/EC; and (iii) applicable national implementations of (i) and (ii) in the EU and EEA member states.

1.5 **"Instructions"** means Customer's written instructions to Staffbase for the processing of Personal Data consisting of the Governing Agreement; any Order Forms; any instructions given by Customer via its use of the Staffbase Service; and any additional instructions mutually agreed by the parties in writing.

1.6 **"Model Clauses"** means the standard contractual clauses for processors approved pursuant to the European Commission's decision 2010/87/EU of 5 February 2010 (**"2010 Model Clauses"**), or any updated, replaced or alternative standard contractual clauses approved by the European Commission such as the standard contractual clauses approved pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 (**"2021 Model Clauses"**).

1.7 **"Personal Data"** means any Customer Data that relates to an identified or identifiable natural person to the extent that such information is protected under Applicable Privacy Law. Personal Data includes, but is not limited to, the Personal Data described in **Exhibit 1**.

1.8 **"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 Staffbase Services.

1.9 **"Sub-Processor"** means any Processor engaged by Staffbase or its Affiliates to assist in fulfilling Staffbase's obligations under the Governing Agreement. Sub-Processors may include third parties or Staffbase Affiliates, and are listed on

https://staffbase.com/en/legal/subprocessors/ (URL: https://staffbase.com/en/legal/subprocessors/) (the **"Sub-Processor Page"**).

1.10 **"Supervisory Authority"** means any independent authority responsible for administering Applicable Privacy Law.

The terms **"Controller"**, **"Data Subject"**, **"Processor"** and **"processing"** will have the meaning given to them under EU Data Protection Law and **"process"**, **"processes"** and **"processed"** will be interpreted accordingly. Any other terms not expressly defined here have the same meanings as in the Governing Agreement.

2 ROLES AND RESPONSIBILITIES.

2.1 **Roles of the Parties.** The parties understand and agree that with regard to the processing of Personal Data, Customer is the Controller and Staffbase is the Processor. Staffbase or its Affiliates may engage Sub-Processors in accordance with the requirements laid down in this DPA. The details of the processing are explained in Exhibit 1.

2.2 **Customer's Processing.** Customer will process Personal Data in accordance with Applicable Privacy Laws and will ensure its Instructions also comply with Applicable Privacy Laws. Between the parties, Customer has sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which it acquires the Personal Data.

2.3 **Staffbase's Processing.** Staffbase will process Personal Data only as described in this DPA, the Governing Agreement, any relevant Order Form and any other written instructions from Customer (the **"Purpose"**). Staffbase will not process the Personal Data for any other Purpose unless: **(i)** as agreed in writing by Customer; or **(ii)** Staffbase is required to do so by applicable law of the Union or the Member States to which Staffbase is subject. In the latter case, Staffbase will notify Customer of such legal requirements prior to the processing, unless the relevant law prohibits such notification on important grounds of public interest. Staffbase will inform Customer without undue delay if, in Staffbase's opinion, any Instruction infringes Applicable Privacy Law. In that case, Staffbase reserves the right to refuse and/or suspend the execution of the Instructions.

3 REQUESTS AND CONSULTATIONS.

3.1 **Data Subject Requests.** Taking into account the nature of processing, Staffbase will provide reasonable assistance to Customer to enable Customer to comply with its obligations with respect to Data Subjects rights

under Applicable Privacy Law. Data Subject rights include, but are not restricted to: access, rectification, restriction, deletion ("right to be forgotten"), objection or portability of Personal Data (each, a **"Data Subject Request"**). If a Data Subject Request is made directly to Staffbase, Staffbase will promptly, to the extent legally permitted, inform Customer. Staffbase will not respond to a Data Subject Request directly without the prior consent of Customer, except as appropriate, for example to direct the Data Subject to Customer. Customer is solely responsible for responding to any Data Subject Requests.

3.2 DPIA. Upon Customer's request and to the extent required under Applicable Privacy Law, Staffbase will provide Customer with reasonable cooperation and assistance to carry out a data protection impact assessment related to Customer's use of the Staffbase Services.

3.3 Consultation by Supervisory Authority. To the extent required under Applicable Privacy Law, Staffbase will provide reasonable assistance to Customer in the cooperation or prior consultation with a Supervisory Authority.

4 SECURITY & CONFIDENTIALITY.

4.1 Confidential Information. Staffbase will handle all Personal Data as Confidential Information as set out in the Governing Agreement.

4.2 Personnel. Staffbase will ensure that its and its Affiliate's employees and contractors who have access to Personal Data are: (i) subject to written obligation to maintain Personal Data as confidential; and (ii) adequately instructed in the good handling of Personal Data. Staffbase will implement measures to restrict employee access to Personal Data as set out in the Security Measures.

4.3 Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subject, Staffbase will implement and maintain appropriate technical and organizational measures, as described in **Exhibit 2** of this DPA (**"Security Measures"**), to ensure a level of security appropriate to the risk. Staffbase regularly monitors compliance with its Security Measures. Staffbase may implement alternative adequate Security Measures from time-to-time while making sure the security level of the defined measures is not reduced.

5 PERSONAL DATA BREACH.

5.1 **Notification.** To the extent required under Applicable Privacy Law, Staffbase will notify Customer without undue delay after it becomes aware of any Personal Data Breach and will provide commercially reasonable cooperation and assistance in identifying the cause of such Personal Data Breach. The notice must include, as available: (i) a description of what happened; (ii) the scope of the Personal Data Breach, including a description of the type of Personal Data involved; (iii) a description of Staffbase's response and any remedial or mitigating measures taken or planned by Staffbase; and (iv) other information as may be reasonably required to be disclosed under applicable Applicable Privacy Laws. Staffbase will provide Customer information that is necessary for the Customer to fulfil its notification and communication obligations, to the extent that information is commercially reasonably available to Staffbase. Staffbase's obligation to report or respond to a Personal Data Breach under this Section is not an acknowledgement by Staffbase of any fault or liability with respect to the Personal Data Breach

5.2 **Cooperation.** Also, Staffbase will take commercially reasonable steps to remedy or mitigate the effects of the Personal Data breach to the extent this is within Staffbase's control. Staffbase may delay its notifications as requested by law enforcement or in light of its legitimate need to investigate or remediate a Personal Data Breach. For security reasons, the parties agree to keep information regarding the Personal Data Breach confidential, unless disclosure is required by law.

6 SUB-PROCESSORS.

6.1 **Appointment of Sub-Processors.** Customer agrees to Staffbase's use of the Sub-Processors listed on the Sub-Processor Page. Staffbase is allowed to appoint additional or replace Sub-Processors provided that Staffbase informs Customer of the identity of the Sub-Processor and the scope of the planned processing. Staffbase will enter into a written agreement with each Sub-Processor containing data protection obligations that provide at least the same level of protection as those in this DPA, to the extent applicable to the nature of the services provided by the Sub-Processor. Customer acknowledges that it may use the Staffbase Service with Third-Party Services, and that these products are not Sub-Processors of Staffbase.

6.2 **Notification of new Sub-Processor.** Staffbase will notify Customer of a new Sub-Processor before authorizing that Sub-Processor to process Personal Data in connection with the Staffbase Services.

6.3 Objection to Sub-Processor. If EU Data Protection Law applies to either party's processing of Personal Data, Customer may object to the engagement of a new Sub-Processor, solely based on reasonable grounds relating to data protection. Customer will inform Staffbase of its objection in writing to privacy@staffbase.com (URL: mailto:privacy@staffbase.com) within 30 calendar days of Staffbase's notification. Customer's notice will contain the reasonable grounds for the objection. The parties agree to discuss Customer's concerns in good faith with the intention to achieve a commercially reasonable solution.

6.4 Non-EEA Sub-Processors. Staffbase will not transfer Personal Data outside the EEA unless it has taken adequate measures to ensure the transfer complies with EU Data Protection Law. Such measures may include, but are not limited to, transferring the Personal Data: **(i)** to a Sub-Processor in a country that has a finding of adequacy from the European Commission; or **(ii)** on the basis of Model Clauses. Where relevant, Customer authorizes Staffbase to conclude the 2010 Model Clauses up to 27 September 2021 with any new Sub-Processor for the processing of the relevant Personal Data, if required. As of 27 September 2021, Staffbase will conclude the 2021 Model Clauses with new Sub-Processors. Staffbase will endeavour to implement the 2021 Model Clauses with all of its Sub-Processors as soon as possible, but in any event before 27 December 2022 in accordance with Article 4 of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

7 AUDITS.

7.1 By Customer. To the extent required under Applicable Privacy Law, Staffbase will make available to Customer all relevant information in Staffbase's possession or control that is necessary to demonstrate compliance with this DPA. Staffbase will also allow for and contribute to audits, including inspections, by Customer (or its appointed third party auditors) in relation to Staffbase's processing of Personal Data. Customer agrees to take all reasonable measures to prevent unnecessary disruption of Staffbase's operations and to exercise its audit rights only once every twelve (12) calendar months, except if: (i) and when required by instruction of a Supervisory Authority; (ii) Customer believes a further audit is necessary due to a Personal Data Breach, or (iii) Customer can provide documented factual grounds for suspicion that Staffbase has breached essential obligations of this DPA. The costs of the audit, including any reasonable costs that Staffbase has to make to cooperate with the audit, will be borne by Customer. Any third party auditor must be suitably qualified, and sign

an appropriate non-disclosure and confidentiality agreement with Staffbase before any audit.

7.2 By Supervisory Authorities. Staffbase will provide Customer or a Supervisory Authority with reasonable access to its documentation and Staffbase's systems in the event of an audit required by a Supervisory Authority, to the extent the audit is required for compliance with Applicable Privacy Laws. The parties will mutually agree on the timing and scope of these audits, which will be: (i) carried out in such a way as to mitigate any disruption to Staffbase's business; and (ii) performed at Customer's sole expense.

7.3 Staffbase Confidential Information. Any executive summaries, audit reports or other audit results will be considered Staffbase's Confidential Information and subject to the "Confidential Information" Section of the Governing Agreement. Staffbase is not required to disclose any commercial secrets, including algorithms, source code, trade secrets and similar information.

8 TERMINATION AND DELETION.

8.1 Return or deletion of Personal Data. Upon expiry of the Subscription Term or termination of the Governing Agreement, Staffbase will delete or return all Personal Data processed under this DPA. This requirement will not apply to the extent Staffbase is obliged by applicable law to retain some or all Personal Data.

8.2 Storage of documentation. Staffbase may maintain documentation to demonstrate compliance with its obligations under this DPA after termination of the Governing Agreement.

9 GENERAL. If Customer and Staffbase have signed a prior data processing agreement, that agreement is hereby terminated and replaced by this DPA as of the date of last signature of the most recent Order Form. If any of Customer's Affiliates is considered the Controller (either alone or jointly with Customer) of Personal Data, Customer is responsible under this DPA for this Personal Data and Affiliate. This DPA is incorporated and part of the Governing Agreement and is subject to all the terms and conditions, including provisions related to limitations of liability, termination, jurisdiction, and governing law of the Governing Agreement.

Exhibit 1 – Personal Data

A. Nature and Purpose of processing

Staffbase will process Personal Data as necessary to provide the Staffbase Services in accordance with the Governing Agreement, as further specified in the Order Form, and as further instructed by Customer in its use of the Staffbase Services.

B. Duration of processing

Staffbase will Process Personal Data for the duration of the Subscription Term, unless otherwise agreed in writing.

C. Categories of Data Subjects

The Personal Data transferred concern the following categories of Data Subjects:

Authorized Users: Users specially designated and authorized by Customer to access the Staffbase Services.
Unregistered Users: Users that access the Public Area that are not Admin Users or Registered Users.

Product-Specific Categories of Data Subjects

If Customer has purchased the Staffbase Service listed below, then the relevant categories of Data Subject are concerned:

Staffbase Service	Categories of Data Subjects
Employee Email	**Employee Email Users:** All users specially designated and authorized by Customer to access and use the Employee Email service. **Email Recipients:** Customer employees and other internal audiences who receive email newsletters from Customer via the Employee Email service.

D. Categories of Personal Data

Customer can submit Personal Data to the Staffbase Services, the extent of which is determined and controlled by Customer, and may contain:

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 comprised in Customer Data, for example a 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

Product-Specific Categories of Personal Data

If Customer has purchased the Staffbase Service listed below, then the relevant categories of Personal Data are processed:

Staffbase Service	Categories of Personal Data
Employee Email	**Account information:** Full name, email address, and password of Employee Email 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.

E. Special Categories of Personal Data (if appropriate)

The Customer may only use the Staffbase Services to process any special categories of Personal Data as specifically permitted by the Service-Specific Terms. 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.

Exhibit 2 – Technical and Organizational Measures

1 SECURITY

1.1 **Security Measures.** Staffbase will maintain the Security Measures described in this Exhibit and may implement additional or alternative Security Measures while making sure the security level of the defined measures is not reduced.

1.2 **ISO 27001.** Staffbase will maintain its ISO/IEC 27001:2013 certification (or equivalent replacement). Customer may download a copy of Staffbase's most recent ISO certificates at https://staffbase.com/en/security/ (URL: https://staffbase.com/en/security/).

1.3 **Employee Email Specific Security: SOC 2.** If Customer has purchased Employee Email, then Staffbase's SOC 2 report (or equivalent replacement) is applicable to Customer's use of Employee Email. Customer may request a copy of Staffbase's most recent SOC 2 report. Customer agrees and acknowledges that the Staffbase ISO/IEC 27001:2013 certification is not (yet) applicable to Employee Email.

2 ACCESS CONTROLS

2.1 **Physical Access Control**. Staffbase will take reasonable measures to prevent unauthorized persons from gaining physical access to Personal Data. Security Measures include but may not be limited to:

(a) The application is hosted in ISO 27001 certified data centers. Physical access to these data centers is highly restricted.

(b) Staffbase's offices are secured and access to the Staffbase offices is limited to Staffbase employees and authorized cleaning services. Employees and cleaning services receive access media (like keys and key cards). Guests are welcomed at the door and accompanied to the contact person. The issue and return of the access media is documented in writing.

2.2 **Internal Access Control.** Staffbase will take reasonable measures to prevent unauthorized Staffbase personnel from gaining access to Personal Data. 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.

2.3 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.

2.4 Electronic Access Control. 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 identification and successful authentication by username and password 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) If the workstation or terminal is inactive for more than five minutes, a password-protected screen saver is automatically activated using the built-in mechanisms of the operating system.

(e) Workstations and terminals are protected against unauthorized use when leaving the workstation temporarily (by manually activating the password-protected screen saver or by locking the system).

(f) Passwords are managed by password managers and are generated with a minimum complexity of at least 32 characters as well as a character mix of numbers, special characters and upper-and-lower case letters.

(g) Access to the workstations and password manager is password protected. The password must be at least 10 characters long as well as a character mix of numbers, special characters and upper-and-lower case letters.

2.5 Isolation Control. Staffbases' testing and staging systems are separated logically from production systems. For testing, Staffbase facilitates dedicated test data.

3 PSEUDONYMIZATION & ENCRYPTION

3.1 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.

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

4 INTEGRITY

4.1 Data Transfer Control. Data is transferred exclusively using the encrypted HTTPS protocol.

4.2 Data Entry Control. Customer's activities related to the creation and update of user data records are logged.

5 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 across four countries, 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 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.

6 TESTING, ASSESSMENT AND EVALUATION

6.1 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.

6.2 Training. All employees of Staffbase receive annual security and data protection awareness training.

6.3 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.

Exhibit 3 – CCPA Specific Terms

In the event of any conflict or ambiguity between the CCPA Specific Terms and the terms of this DPA, and only to the extent Staffbase processes any Personal Data protected by the CCPA, these CCPA Specific Terms will prevail.

1. The definitions of: “Controller” includes “Business”; “Processor” includes “Service Provider”; “data subject” includes “consumer”; “Personal Data” includes “Personal Information”; in each case as defined under CCPA.

2. The parties agree that Customer is a Business and Staffbase is a Service Provider when processing personal information in accordance with Customer’s Instructions.

3. Staffbase will process Personal Information only for the purpose of performing the Staffbase Services under the Governing Agreement, for any other Business Purpose (as defined in the CCPA) as allowed under the CCPA, and in accordance with any written instructions from Customer. Staffbase will not: (i) sell Personal Information; (ii) retain, use or disclose personal information for a commercial purpose other than for the Business Purpose or otherwise permitted by the CCPA; or (iii) retain, use, or disclose Personal Information outside of the direct business relationship between Customer and Staffbase.

4. Staffbase and Customer acknowledge and agree that Staffbase is not “selling” Personal Data to its authorized Sub-Processors in connection with the provision of the Service.

5. Staffbase’s obligations regarding Data Subject Requests under this DPA apply to consumer’s rights under the CCPA to the extent applicable under the CCPA.

6. Staffbase certifies that it understands and will comply with the restrictions set out in this Exhibit 3.