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This is an archived version of the Staffbase Data Processing Agreement.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/).

19 March 2020

This Staffbase Data Processing Agreement (**"DPA"**) forms part of the Staffbase Terms of Service (URL: https://staffbase.com/en/terms/) (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: (i) EU Data Protection Law; (ii) 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European Union; and (iii) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case as amended, repealed, superseded or replaced from time to time.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 **"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.

1.4 **"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.

1.5 **"Model Clauses"** means the standard contractual clauses for processors approved pursuant to the European Commission's decision 2010/87/EU of 5 February 2010, or any updated standard contractual clauses approved by the European Commission.

1.6 **"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**.

1.7 **"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.

1.8 **"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 Exhibit 2.

1.9 **"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) as required by applicable law. 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 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.

4.2 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 3 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. 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 (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 in **Exhibit 2**. 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 Objection to Sub-Processor. Customer may object in writing to Staffbase's appointment of a new Sub-Processor within 30 calendar days after receipt of Staffbase's notification in accordance with Section 6.1. If Customer objects, it will inform Staffbase in writing of the reasonable grounds relating to data protection for the objection. The parties agree to discuss Customer's concerns in good faith with the intention to achieve a commercially reasonable solution.

6.3 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. With regard to Model Clauses, Customer authorizes Staffbase to conclude Model Clauses with a Sub-Processor for the processing of the relevant Personal Data, if required.

7 AUDITS.

7.1 By Customer. 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 as an attachment to 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:

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

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:

x	**Profile information:** User profile information, such as name, email address, position, department and location and other required or voluntary profile information.
x	**Login data:** Email and password
x	**Content:** Any other Personal Data comprised in Customer Data, for example a Personal Data in chats or in media files.
x	**Technical information:** Device type, IP address, User ID, operation system, browser type, user agent, timestamp of visits and local storage

E. Special Categories of Personal Data (if appropriate)

The Customer may not use the Staffbase Services to process any special categories of Personal Data unless specifically permitted by the Governing Agreement or the Service-Specific Terms.

Exhibit 2 – Sub-Processors

List of authorized sub-processors according to Section 6:

This Exhibit contains a list of current Sub-Processors that are engaged in processing Personal Data to the extent as mentioned below. Controller agrees to the commissioning of these Sub-Processors, which may be amended from time to time according to the conditions in Section 6.

Service Provider	**Country and Address**	**Processing Activities**	**Storage Location**
Infrastructure – DE Hosting			
1&1 IONOS SE	Elgendorfer Str. 57, 56410 Montabaur, Germany	ISO 27001 certified data hosting.	Germany
SysEleven GmbH	Boxhagener Straße 80, 10245 Berlin, Germany	ISO 27001 certified data hosting.	Germany
Infrastructure – US Hosting			
In addition to the above, we use the following Sub-Processor for Customers with US hosting			
Microsoft Corporation (Azure)	One Microsoft WayRedmond, Washington 98052, USA	ISO 27001 certified data hosting.	USA
Other Staffbase Service functions			
Mailjet SAS	13-13 bis, rue de l'Aubrac – 75012 Paris, France	ISO 27001 certified email service provider used to deliver emails to Authorized Users. Mailjet has access to the email addresses of Authorized Users and the content of the email itself.	EU
Zendesk, Inc.	1019 Market Street, San Francisco, CA 94103, USA	Zendesk provides a platform to manage customer support requests. Only Admin Users can request support from Staffbase via the Zendesk platform. The Personal Data that may be processed by Zendesk in this regard is the Admin User's name, email address and content of the support ticket.	EU
Optional Sub-Processors			

Amazon Web Services Inc.*	410 Terry Avenue North, Seattle, Washington 98109-5210, USA	Amazon provides a Content Delivery Network (CDN) for international distribution of any media asset (pictures, video, files) selected for use with the Staffbase Service. Customer's use of the CDN results in faster delivery of media files. Media files uploaded by Customer can contain Personal Data, such as names or images. * If the CDN service is turned off, Amazon Web Services Inc. is not a Sub-Processor.	Global
Microsoft Corporation*	One Microsoft Way Redmond, Washington 98052, USA	ISO 27001 certified translation service. We use Microsoft Translator to provide on-demand translations. Microsoft may process Personal Data stored in the content of what is sent for translation. Microsoft immediately deletes this information and so no translations are written to permanent storage. There will be no record of the submitted content, or portion thereof, in any Microsoft data center. * If the translation service is turned off or not available for the end user, Microsoft Corporation is not a Sub-Processor.	EU

Staffbase Group

Depending on the geographic location of a Customer or their Admin Users, and the type of Staffbase Services provided, Staffbase may also engage one or more of the following Staffbase Affiliates as Sub-Processors when accessing Customer Data:

Staffbase Affiliate	Affiliate details
Staffbase UK Ltd.	**UK** – Registered in England with Company number 11666265
Staffbase B.V.	**Netherlands** – Registered in the Netherlands with Company number 75849895
Staffbase Inc.	**USA** – Incorporated in Delaware, US, with file number 6032180, with headquarters in New York, New York.

These Staffbase Affiliates may deliver (customer) support and similar services to a Customer. For example, our customer support team of Staffbase Inc. may need to provide support to a Customer that has entered into the Agreement with Staffbase GmbH. Staffbase has an intragroup data processing agreement, including Standard Contractual Clauses, to facilitate these transfers.

Exhibit 3 – Technical and Organizational Measures

1. CONFIDENTIALITY.

Physical Access Control

No unauthorised access to data processing facilities, e.g., magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm

systems, video/CCTV Systems.

The hosting of the application is carried out by the Sub-Processors listed in Exhibit 2.

The desktop computer/personal computers belonging to Staffbase are located in locked offices. Access to these offices is limited to the employees and the cleaning service. Employees and the cleaning service receives access media (keys, key cards, etc.). Guests are welcomed at the door and accompanied to the contact person.

The issue and return of the access media is documented in writing. There is a security agreement with the cleaning service provider.

Electronic Access Control
No unauthorised use of the data processing and data storage systems, e.g., (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media.

Access to the data processing system is only possible after identification and successful authentication by username and password using state-of-the-art security measures. Access is accordingly denied in the absence of authorization.

The circle of persons authorized to access data processing systems on which data is processed and/or stored is limited to the minimum necessary for the respective task or function fulfilment. 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 media and/or user ID/password combinations will not be passed on to third parties.

Authentication codes for temporarily employed persons (external developers, interns, trainees) are allocated individually. No reusable IDs (e. g. trainee1, etc.) are assigned.

A process for requesting, approving, issuing and withdrawing authentication media and access authorizations has been set up and documented, and is being applied.

Automatic access blocking: 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.

Manual access blocking: 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).

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.

Access to the workstations and password manager is password protected. The password must be at least 10 characters long.

Internal Access Control (permissions for user rights of access to and amendment of data)
No unauthorised reading, copying, changes or deletions of Personal Data within the system, e.g., rights authorisation concept, need-based rights of access, logging of system access events.

A select number of Staffbase employees have access to Customer Data in the following roles:

- 3rd Level – System administrator: Personal access to all data within the corresponding customer instance including database.
- 2nd Level – Support Administration: Personalized access to all data within the associated customer instance, but no server/database access.
- 1st Level – Customer Success Access: Access to all data within a customer instance through the application according to the Customer's approval. The administrator defines the rights of the account (app-admin, editor, user, etc.) at the application level. No access to databases as well as login data (email and password) of the individual users is available. The support access is not person-specific and is available to all members of the Customer Success/Support Team.

The roles have only the minimum number of staff members of Staffbase. The allocation of access is recorded and reviewed at least once a year.

Isolation Control
The isolated processing of data, which is collected for differing purposes, e.g., multiple customer support, sandboxing.

Test and production data are separated, and development, staging, and production instances are separated.

Pseudonymisation & Encryption
The processing of Personal Data in such a method/way that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that

this additional information is stored separately and is subject to appropriate Security Measures.

Encryption: All communication between server and clients is encrypted according to the state of the art.

Pseudonymization: With selected plugins it is also possible to pseudonymize the data during processing.

2. INTEGRITY.

Data Transfer Control
No unauthorised reading, copying, changes or deletions of Data with electronic transfer or transport, e.g., encryption, Virtual Private Networks (VPN), electronic signature.

Data is transferred exclusively using the encrypted HTTPS protocol.

Data Entry Control
Verification, whether and by whom Personal Data is entered into a data processing system, is changed or deleted, e.g., logging, document management.

The time and identity of the admin is logged when creating and changing user data records.

3. AVAILABILITY & RESILIENCE.

Availability Control
Prevention of accidental or wilful destruction or loss, e.g., backup strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning.

Staffbase ensures a daily backup of the data. The backup of the data is kept for 30 days.

Rapid Recovery
The recovery of backup data in an emergency is tested and improved during annual training session.

4. REGULAR 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 data protection officer.

Training/Commitment
All employees of Staffbase who handle Personal Data are documented to be trained in the following subjects:

- Principles of data protection, including technical and organisational measures
- Obligation to maintain confidentiality regarding trade and business secrets, including Customer's transactions
- Proper and careful handling of data, files, data carriers and other documents
- Secrecy of telecommunications
- Obligation to maintain confidentiality and privacy (written)

The instruction is repeated at least every three years, but also at shorter intervals if necessary (e.g., change of order circumstances or legal regulations).

Incident Response Management
Staffbase will inform Customer without undue delay about cases of serious operational disturbances and Personal Data Breaches if errors are detected or other irregularities in the handling of data of Customer. Staffbae will remedy this immediately.

Data Protection by Design and Default
The employee app only collects, stores or processes data that is at most necessary for fulfilling the task or execution of the proces

Order or Contract Control
The persons authorised 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 account manager and staff members of the Staffbase customer success/support team.

Instructions from Customer are generally accepted and confirmed in writing. Verbally received Customer instructions must be confirmed by Customer in writing without delay within a maximum of 3 working days.

Regulations/restrictions on order execution: Only those works that are included in the specifications are carried out. All other work steps going beyond this must first be agreed with the competent authority on the part of Customer and approved in writing. Staffbase agrees in advance with Customer on the schedule of the execution of the order.