DATA PROCESSING AGREEMENT
PITCH SOFTWARE GMBH

1. Subject of the Agreement

In the course of the fulfillment of the contract between Pitch Software GmbH, Joachimstraße 7, 10119 Berlin (the "**Processor**") and the customer (the "**Customer**", together with the Processor the "**Parties**") regarding the provision of the Processor's software to the Customer (the "**Contract**"), it is possible that the Processor deals with personal data pursuant to Art. 4 no. 1 General Data Protection Regulation ("**GDPR**"), i.e. any information relating to an identified or identifiable natural person (e.g. names, addresses or phone numbers of persons who are the Customer's customers), with regard to which the Customer acts as a controller pursuant to data protection law (the "**Customer Data**"). This agreement (the "**Agreement**") specifies the data protection obligations and rights of the Parties in connection with the Processor's use of Customer Data to render the services under the Contract.

2. Scope of the Processing

2.1 The Processor shall process the Customer Data on behalf and in accordance with the instructions of the Customer within the meaning of Art. 28 GDPR. The Customer remains the controller pursuant to Art. 28 GDPR.

2.2 The processing of Customer Data by the Processor occurs in the manner and the scope and for the purpose determined in **Annex 2.2** to this Agreement; the processing relates to the types of personal data and categories of data subjects specified therein. The duration of processing corresponds to the term of the Contract.

2.3 The Processor reserves the right to anonymize or aggregate the Customer Data in such a way that it is no longer possible to identify individual data subjects, and to use them in this form for the purpose of needs-based designing, machine-learning, developing and optimizing as well as rendering of the services agreed as per the Contract. The Parties agree that anonymized and according to the above requirement aggregated Customer Data are not considered Customer Data for the purposes of this Agreement.

2.4 The Processor may process and use the Customer Data for the Processor´s own purposes as controller to the extent legally permitted by data protection law, if permitted by a statutory permission or consent by the data subject. This Agreement does not apply to such data processing.

2.5 The processing of Customer Data by the Processor shall in principle take place inside the European Union or another contracting state of the European Economic Area (EEA). The

Processor is nevertheless permitted to process Customer Data in accordance with the provisions of this Agreement outside the EEA if the Processor informs the Customer in advance (e.g. in the privacy policy) about the place of data processing and if the requirements of Art. 44 to 48 GDPR are fulfilled or if an exception according to Art. 49 GDPR applies.

3. Right of the Customer to Issue Instructions

3.1 The Processor processes the Customer Data in accordance with the instructions of the Customer, unless the Processor is legally required to do otherwise. In the latter case, the Processor shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.2 The instructions of the Customer are in principle conclusively stipulated and documented in the provisions of this Agreement. Individual instructions which deviate from the stipulations of this Agreement or which impose additional requirements shall require the Processor's consent.

3.3 The Processor shall ensure that the Customer Data is processed in accordance with the instructions given by the Customer. If the Processor is of the opinion that an instruction given by the Customer infringes this Agreement or applicable data protection law, the Processor is after correspondingly informing the Customer entitled to suspend the execution of the instruction until the Customer confirms the instruction. The Parties agree that the sole responsibility for the processing of the Customer Data in accordance with the instructions lies with the Customer.

4. Legal Responsibility of the Customer

4.1 The Customer is solely responsible for the permissibility of the processing of the Customer Data and for safeguarding the rights of data subjects in the relationship between the Parties. Should third parties assert claims against the Processor based on the processing of Customer Data in accordance with this Agreement, the Customer shall indemnify the Processor from all such claims upon first request.

4.2 The Customer is responsible to provide the Processor with the Customer Data in time for the rendering of services according to the Contract and the Customer is responsible for the quality of the Customer Data. The Customer shall inform the Processor immediately and completely if during the examination of the Processor's results the Customer finds errors or irregularities with regard to data protection provisions or instructions of the Customer.

4.3 Upon request, the Customer shall provide the Processor with the information specified in Art. 30 para. 2 GDPR, insofar as it is not already available to the Processor.

4.4 If the Processor is required to provide information to a governmental body or person on the processing of Customer Data or to cooperate with these bodies in any other way, the Customer is obliged to assist the Processor at first request in providing such information and in fulfilling other appropriate cooperation obligations.

5. Requirements for Personnel and Systems

The Processor shall commit all persons engaged in processing Customer Data to confidentiality with respect to the processing of Customer Data.

6. Security of Processing

6.1 The Processor takes necessary appropriate technical and organizational measures according to Art. 32 GDPR, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the Customer Data, as well as the different likelihood and severity of the risk to the rights and freedoms of the data subjects, in order to ensure a level of protection of Customer Data appropriate to the risk. The implemented technical and organizational measures include the measures as listed in **Annex 6.1**.

6.2 The Processor shall have the right to modify technical and organizational measures during the term of this Agreement, as long as they continue to comply with the statutory requirements.

7. Engagement of Further Processors

7.1 The Customer grants the Processor the general authorization to engage further processors with regard to the processing of Customer Data. Further processors engaged at the time of conclusion of this Agreement are listed in **Annex 7.2**. In general, no authorization is required for contractual relationships with service providers that are concerned with the examination or maintenance of data processing procedures or systems by third parties or that involve other additional services, even if access to Customer Data cannot be excluded, as long as the Processor takes reasonable steps to protect the confidentiality of the Customer Data.

7.2 The Processor shall notify the Customer of any intended changes in relation to the consultation or replacement of further processors. In individual cases, the Customer has the right to object to the engagement of a potential further processor. An objection may only be raised by the Customer for important reasons which have to be substantiated vis-à-vis the Processor. Insofar as the Customer does not object within 14 days after receipt of the notification, the Customer´s right to object to the corresponding engagement lapses. If the Customer objects, the Processor is entitled to terminate the Contract and this Agreement with a notice period of three months until the end of a month.

7.3 The agreement between the Processor and the further processor must impose the same obligations on the further processor as those incumbent upon the Processor under this Agreement. The Parties agree that this requirement is fulfilled if the contract has a level of protection corresponding to this Agreement.

7.4 Subject to compliance with the requirements of Sec. 2.5 of this Agreement, the provisions of this Sec. 7 shall also apply if a further processor in a third country is involved. The Customer hereby authorises the Processor to conclude an agreement with another

processor on behalf of the Customer based on the standard contractual clauses for the transfer of personal data to processors in third countries pursuant to the decision of the European Commission of February 5th in 2010. The Customer declares its willingness to cooperate in fulfilling the requirements of Art. 49 GDPR to the extent necessary.

8. Data Subjects' Rights

8.1 The Processor shall support the Customer within reason by virtue of technical and organisational measures in fulfilling the Customer's obligation to respond to requests for exercising data subjects' rights.

8.2 As far as a data subject submits a request for the exercise of its rights directly to the Processor, the Processor will forward this request to the Customer in a timely manner.

8.3 The Processor shall inform the Customer of any information relating to the stored Customer Data, about the recipients of Customer Data to which the Processor may disclose it in accordance with the instructions and about the purpose of storage, as far as the Customer does not have this information at its disposal and as far as the Customer is not able to collect it itself.

8.4 The Processor shall, within the bounds of what is reasonable and necessary, enable the Customer to correct, delete or restrict the further processing of Customer Data, or at the instruction of the Customer correct, block or restrict further processing itself, if and to the extent that this is impossible for the Customer. In this case, the Processor shall be reimbursed for the expenses and costs incurred by the Processor in this regard and substantiated vis-à-vis the Customer.

8.5 Insofar as the data subject has a right of data portability vis-à-vis the Customer in respect of the Customer Data pursuant to Art. 20 GDPR, the Processor shall support the Customer within the bounds of what is reasonable and necessary in handing over the Customer Data in a structured, commonly used and machine-readable format, if the Customer is unable to obtain the data elsewhere. In this case, the Processor shall be reimbursed for the expenses and costs incurred by the Processor in this regard and substantiated vis-à-vis the Customer.

9. Notification and Support Obligations of the Processor

9.1 Insofar as the Customer is subject to a statutory notification obligation due to a breach of the security regarding the Customer Data (in particular pursuant to Art. 33, 34 GDPR), the Processor shall inform the Customer in a timely manner of any reportable events in the Processor´s area of responsibility. The Processor shall assist the Customer in fulfilling the notification obligations at the Processor's request to the extent reasonable and necessary. In this case, the Processor shall be reimbursed for the expenses and costs incurred by the Processor in this regard and substantiated vis-à-vis the Customer.

9.2 The Processor shall assist the Customer to the extent reasonable and necessary with data protection impact assessments to be carried out by the Customer and, if necessary, subsequent consultations with the supervisory authority pursuant to Art. 35, 36 GDPR. In

this case, the Processor shall be reimbursed for the expenses and costs incurred by the Processor in this regard and substantiated vis-à-vis the Customer.

10. Deletion and Return of Customer Data

10.1 Upon termination of this Agreement, the Processor shall, in the discretion of the Customer,

a) either delete or return the Customer Data; and

b) delete existing copies thereof

unless the Processor is obligated by law to further store the Customer Data.

10.2 The Processor may keep documentations which serve as evidence of the orderly and accurate processing of Customer Data, also after the termination of this Agreement.

11. Evidence and audits

11.1 The Processor shall provide the Customer, at the Customer's request, with all information required and available to the Processor to prove compliance with its obligations under this Agreement.

11.2 The Customer shall be entitled to audit (including inspections) the Processor with regard to compliance with the provisions of this Agreement, in particular the implementation of the technical and organisational measures.

11.3 In order to carry out inspections in accordance with Sec. 11.2., the Customer is entitled to access the business premises of the Processor in which Customer Data is processed within the usual business hours (Mondays to Fridays from 10 am to 6 pm) after timely advance notification in accordance with Sec. 11.5 at its own expense, without disruption of the course of business and under strict secrecy of the Processor's business and trade secrets.

11.4 The Processor is entitled, at its own discretion and taking into account the Customer's legal obligations, not to disclose information which is sensitive with regard to the Processor's business or if the Processor would be in breach of statutory or other contractual provisions as a result of its disclosure. The Customer is not entitled to get access to data or information about the Processor's other customers, cost information, quality control and contract management reports, or any other confidential data of the Processor that is not directly relevant for the agreed audit purposes.

11.5 The Customer shall inform the Processor in good time (usually at least two weeks in advance) of all circumstances in relation to the performance of the audit. The Customer may carry out not more than one audit per calendar year.

11.6 If the Customer commissions a third party to carry out the audit, the Customer shall obligate the third party in writing in the same way as the Customer is obliged vis-à-vis the Processor according to this Sec. 11. In addition, the Customer shall by way of written agreement obligate the third party to maintain secrecy and confidentiality unless the third party is

subject to a professional obligation of secrecy. At the request of the Processor, the Customer shall immediately submit to the Processor the commitment and confidentiality agreements with the third party. The Customer may not commission any of the Processor's competitors to carry out the audit.

11.7 At the discretion of the Processor, proof of compliance with the obligations under this Agreement may be provided, instead of an inspection, by submitting an appropriate current opinion or report from an independent authority (e.g. auditor, audit department, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certification by IT security or data protection audit (the "**Audit Report**"), if the Audit Report makes it possible for the Customer in an appropriate manner to convince itself of the Processor's compliance with the contractual obligations contained in this Agreement.

12. Contract term and termination

The term and termination of this Agreement shall be governed by the term and termination provisions of the Contract. A termination of the Contract automatically results in a cancellation of this Agreement. An isolated termination of this contract is excluded.

13. Liability

13.1 The Processor's liability under this Agreement shall be governed by the disclaimers and limitations of liability provided for in the Contract. As far as third parties assert claims against the Processor which are caused by the Customer's culpable breach of this Agreement or one of the Customer´s obligations as the controller in terms of data protection law, the Customer shall upon first request indemnify and hold the Processor harmless from these claims.

13.2 The Customer undertakes to indemnify the Processor upon first request against all possible fines imposed on the Processor corresponding to the Customer's part of responsibility for the infringement sanctioned by the fine.

14. Final provisions

14.1 In case individual provisions of this Agreement are ineffective or become ineffective or contain a gap, the remaining provisions shall remain unaffected. The Parties undertake to replace the ineffective provision by a legally permissible provision which comes closest to the purpose of the ineffective provision and that thereby satisfies the requirements of Art. 28 GDPR.

14.2 In case of conflicts between this Agreement and other arrangements of the Parties, in particular the Contract, the provisions of this Agreement shall prevail.

Annex 2.2
Further Information on the Processing of Customer Data

1	Purpose and extent of Data Processing	Provision of the Pitch software as a web application, desktop application, or mobile application, and which functions as a platform for creating, collaborating, and distributing of presentations; fulfilment of the Processor's obligations under the Contract.
2	Types of personal data	Contact data; usage data; any data filled in by the Customer in the Software; Employee Data; Customer Data; Supplier Data; User-generated Data; User data; Profile data; Usernames; password; email; logfiles.
3	Categories of data subjects	Users of the Pitch software; possibly other data subjects mentioned or included in data filled in by the Customer in the Software.

Annex 6.1
Technical and Organizational Measures according to Art. 32 GDPR

According to Art. 32 GDPR controller and processor of personal data must take technical and organizational measures (TOM) to ensure that the security and protection requirements of data protection are met. **Technical measures** are to be understood as all protection attempts that are physically implementable in the broadest sense, such as securing doors and windows or measures implemented in software and hardware, such as setting up a user account and password requirement. **Organizational measures** are to be understood as protection attempts that are implemented through instructions, procedures and procedures.

No.	Category of Measures	Description of Category	Technical Measures	Organisational Measures
1	**Encryption (Art. 32 (1) a) GDPR)**	Cryptographic measures to ensure that information is hashed when transferred internally or externally and can only become readable again by using the correct encryption key.	Encryption of the company website (“data in motion”)	
			Encryption of data carriers on laptops/notebooks and mobile data carriers ("data at rest”)	
2	**Confidentiality – physical access control (Art. 32 (1) b) GDPR)**	Measures to prevent unauthorised persons from gaining access to data Processing systems with which personal data is processed or used.	Security of the buildings, windows and doors with an alarm system	Digital keys management system
			Automated access control system and manual locking system with safety locks	
			Light barriers/motion detectors	
			Video surveillance of entrances	
3	**Confidentiality – data access control (Art. 32 (1) b) GDPR)**	Measures to prevent data Processing systems from being used without authorisation.	Authentication with username /password, and/or biometric methods	Allocate user rights, defining user profiles, assignment passwords, and assign user profiles to IT-systems
			Use of Intrusion-Detection-Systems	Immediate blocking of authorization

No.	Category of Measures	Description of Category	Technical Measures	Organisational Measures
				when employees leave the company
			Locked housings / security locks	
			Password protected screensavers and automated screen locking in case of inactivity, and two-factor user authentication	
			Implementation of virtual networks for the separation of data streams	
4	**Confidentiality – data usage control (Art. 32 (1) b) GDPR)**	Measures to ensure that persons entitled to use a data Processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, altered or removed without authorisation in the course of Processing or use and after storage.	Use of document shredders or appropriate service providers and physical deletion of data mediums before reuse	Development of an authorization concept (Differentiated authorisations for read, edit or delete data) and password procedures (incl. special characters, minimum length, change of password)
				Assignment of rights by system administrator
5	**Confidentiality – transmission control (Art. 32 (1) b) GDPR)**	Measures to ensure that personal data cannot be read, copied, altered or removed during electronic transmission or transport or storage onto data carriers, and that it is possible to check and	Documentation of all interfaces	Documentation of recipients of data and the time periods of planned surrender or agreed erasure time limits

No.	Category of Measures	Description of Category	Technical Measures	Organisational Measures
		establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.		
6	**Confidentiality – separation control (Art. 32 (1) b) GDPR)**	Measures to ensure that data collected for different purposes can be processed separately.	Segregation of functions (production/testing)	Development of an authorization concept
			Separated databases and separate tables within database	Logical client separation
7	**Integrity – input control (Art. 32 (1) b) GDPR)**	Full documentation of data management and maintenance must be maintained - to ensure the ongoing integrity of data. Measures for subsequent checking whether data has been entered, changed or removed (deleted), and by whom.	No local admin privileges	Assignment of authorisations for input
				Alteration and erasure of data on the basis of an authorisation concept
8	**Availability – availability control (Art. 32 (1) b) GDPR)**	Measures to ensure that personal data is protected from accidental destruction or loss.	Air conditioning in server rooms	Alarm during unauthorized entry into server room
			Fire extinguishers in server rooms, installation of fire and smoke detection systems, uninterruptible power supply (UPS)	Remote data backup in secure outsourced locations
			Monitoring of temperature and humidity and power outlet strip with surge protection in server rooms	Development of an emergency plan and a disaster recovery plan, in flood areas: server rooms above waterline

No.	Category of Measures	Description of Category	Technical Measures	Organisational Measures
				Server room not under sanitary facilities
9	**Availability – job control (Art. 32 (1) b) GDPR)**	Measures to ensure that, in the case of commissioned Processing of personal data, the data is processed only in accordance with the instructions of the Controller.		Selection of the Processor giving consideration to diligence aspects (in particular with respect to data security)
				Contractual penalties for breaches
				Written instructions to the Processor (e.g. Data Processing Agreement) as defined in Art. 28 (2) GDPR
				Processor has appointed a Data Protection Officer
				Efficient rights of control agreed with the Processor
				Putting the Processor's employees under an obligation of data confidentiality (Art. 28 Abs. 3 lit. b GDPR)
				Assurance of deletion of the data at the end of the provision of services, continuous control of the Processor and its activities

No.	Category of Measures	Description of Category	Technical Measures	Organisational Measures
				Use of Subcontractors requires the Controller's consent and prior verification and documentation of the security measures taken by the Processor
10	**Resilience (Art. 32 (1) b) GDPR)**	Measures to ensure the resilience of the systems and services that guarantee that the systems and services are designed in such a way that even high peak loads and high continuous loads of Processing can be handled.		Testing of storage, access and line capacities
11	**Restoration of availability (Art. 32 (1) c) GDPR)**	Measures to ensure that availability of and access to the data can be restored in a timely manner in the event of a physical or technical incident.	Redundant design of the infrastructure (of hard disks, e.g. RAID)	Backup concept
			Cloud Service	Testing of data restoration
12	**Data protection management (Art. 32 (1) d) GDPR)**	Measures to ensure a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the Processing.		Checking of the DSB and the IT revision

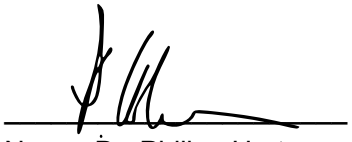
Annex 7.2
Further Processors

No.	Name of the further processor	Description of processing via this further processor
1	Amplitude Inc., 501 2nd Street, Suite 100, San Francisco, CA 94107, USA	Analysis of in-product behaviour
2	Auth0, Inc., 10800 NE 8th Street Suite 600, Bellevue, WA 98004, USA	Authentication software
3	Amazon Web Services Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, USA.	Secure cloud service platform for database storage
4	Bugsnag Inc., 110 Sutter St, Suite 1000, San Francisco, CA 94104, USA	Application stability monitoring software
5	Calendly LLC, 1315 Peachtree St NE, Atlanta, GA 30309, USA	Meeting booking software
6	Product Pains Inc. (Canny.io), 831 N Tatnall Street Suite M #140 Wilmington, DE 19801, USA	In app user feedback tracking software
7	Datadog, Inc., 620 8th Avenue, Floor 45, New York, NY 10018, USA	Application performance management
8	NomNom Insights Ltd, (EnjoyHQ), 9th Floor, 107 Cheapside, London, England EC2V 6DN	User feedback collection and tracking software
9	Falcon.io ApS H.C. Andersens Boulevard 27, 1., 1553, Copenhagen V, Denmark	Social media management software
10	Google Ireland (Google Drive), Gordon House, Barrow Street, Dublin 4, Ireland	Cloud storage for documents
11	Google Ireland (Google Mail), Gordon House, Barrow Street, Dublin 4, Republic of Ireland	Cloud-based email client
12	Hotjar Ltd, Level 2, St Julian's Business Centre, 3, Elia Zammit Street, St Julian's STJ 1000, Malta	Users' behavior visualization software
13	Intercom, 2nd Floor, Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Republic of Ireland	Help and support widget in app
14	Mailchimp, The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	Email marketing automation software
15	Notion, 2948 20th St, Apt. 300 San Francisco, CA 94110, USA	Documentation and notes storage software
16	PushMetrics, August-Bebel-Str. 89 14482 Potsdam, Germany	Managed service version of Apache SWuperset
17	Slack, 500 Howard Street, San Francisco, CA 94105, USA	Team communication and collaboration software

No.	Name of the further processor	Description of processing via this further processor
18	Stripe Inc., 510 Townsend Street San Francisco, CA 94103, USA	Online payment processing and billing software
19	Superhuman Labs, Inc., 465 California Street #1200 San Francisco, CA 94104, USA	Email client
20	TYPEFORM SL, C/Bac de Roda, 163 (Local), 08018 – Barcelona (Spain)	Survey software
21	Zoom Video Communications, Inc., 55 Almaden Blvd. Suite 600, San Jose, CA 95113, USA	Video conferencing software

Signature Page

For the Processor:



Name: Dr. Philipp Hartmann
Function: COO
Date: 15. Nov 2019

For the Customer:

Name:
Function:
Date:

Please contact us on privacy@pitch.com should you have any questions.