# Vereinbarung zur Auftragsverarbeitung (AVV)

*Data Processing Agreement (DPA)*

zwischen
*between*

***Universität Bremen, Bibliothekstraße 1, 28359 Bremen***

– Verantwortlicher – nachstehend "Auftraggeber" genannt
*– the Controller – hereinafter referred to as the "Client"*

und
*and*

**Conceptboard Cloud Service GmbH, Mansfelder Str. 56,**
**06108 Halle (Saale), Germany**

– Auftragsverarbeiter – nachstehend "Conceptboard Gesellschaft" oder "Auftragnehmer"
*– the Processor – hereinafter referred to as "Conceptboard Company" or "Supplier"*

**Wichtiger Hinweis:** Es gilt ausschließlich die deutsche Fassung dieses Vertrags, und in keinem Fall darf die englische Sprachfassung dieses Vertrags dahingehend ausgelegt werden, dass sie die deutsche Fassung dieses Vertrags ändert oder auf andere Weise die Beziehung der Ver- tragspartner untereinander regelt.

***Important Note:*** *The German version of this document will govern our relationship. An English translation is provided for convenience only and will not be interpreted to modify the German version.*

## 1 Gegenstand und Dauer

### 1.1 Gegenstand

(1) Der Gegenstand des Auftrags ergibt sich aus dem Conceptboard Nutzungsvertrag zwischen Auftragnehmer und Auftraggeber, der entweder als Individualvertrag geschlossen wurde oder im Rahmen der Conceptboard Nutzungsbedingungen vom 25. Mai 2018[1] vorliegt (im Folgenden Hauptvertrag).

### 1.2 Dauer

(1) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

(2) Soweit der Regelungsgehalt einzelner Regelungen über die Laufzeit dieser Vereinbarung hinausgeht, bleiben die entsprechenden Verpflichtungen von der Beendigung dieser Vereinbarung unberührt. Dies gilt insbesondere für die Verpflichtung zur Löschung von Daten und der Rückgabe von Datenträgern.

## 2 Konkretisierung des Auftragsinhalts

### 2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

#### 2.1.1 Erhebung und Verwendung von Daten

(1) Die Conceptboard Gesellschaft stellt Dienste für die Online-Zusammenarbeit zwischen Computernutzern bereit. Personenbezogene Daten werden dabei im Rahmen der Registrierung, bei der Nutzung der Dienste und beim Besuch der Webseiten abgefragt. Die personenbezogenen Daten werden verwendet, um die Dienste anzubieten, die Dienste zu verbessern, für anonyme Statistiken und für die Kommunikation mit den Nutzern. Dies wird von

## 1 Subject matter and duration

### 1.1 Subject matter

(1) The Subject matter of the Order or Con- tract results from the Conceptboard usage contract between the contractor and the client, which was either concluded as an individual contract or is available within the framework of the Conceptboard terms of use of May 25, 2018 (hereinafter referred to as Main Contract).

### 1.2 Duration

(1) The duration of this Order or Contract corresponds to the duration of the Main Contract.

(2) Insofar as the regulatory content of individual regulations extends beyond the term of this agreement, the corresponding obligations remain unaffected by the termination of this agreement. This applies in particular to the obligation to delete data and return data carriers.

## 2 Specification of the Order or Contract Details

### 2.1 Nature and Purpose of the intended Processing of Data

#### 2.1.1 Collection and use of data

(1) The Conceptboard Company offers services for online collaboration between computer users. In doing so, personal data is requested and collect while registering for the services, using the services and visiting the web sites. The personal information is used to operate the services, to improve the services, for anonymous statistics, and for communication with the users. This is done by the Conceptboard

[1] https://conceptboard.com/terms/

der Conceptboard Gesellschaft selbst oder beauftragten Dienstleistern übernommen. Zur Dienstverbesserung werden ausschließlich anonymisierte Nutzungsdaten verwendet.

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau wird in diesen Fällen durch einen Angemessenheitsbeschluss der EU-Kommission oder auf der Grundlage besonderer Garantien, wie z.B. vertraglicher Verpflichtung durch sogenannte Standardschutzklauseln der Kommission, des Vorliegens von Zertifizierungen oder verbindlicher interner Datenschutzvorschriften, festgestellt.

**2.1.2 Datenfreigabe zwischen Nutzern**

(1) Die Zusammenarbeit in Conceptboard erfolgt auf interaktiven Arbeitsbereichen (die „Boards"). Nutzer können Daten auf diese Boards transferieren. Wenn ein Nutzer ein Board mit anderen Nutzern teilt, dann werden manche dieser Daten (z.B. Nutzernamen, deren Profil-Bilder, beigetragene Inhalte, Informationen über Zeitpunkte der Mitwirkung) ebenfalls geteilt, um die Zusammenarbeit zu ermöglichen.

(2) Auf die Datenfreigabe zwischen Nutzern hat der Auftragnehmer keinen Einfluss.

**2.2 Art der Daten**

(1) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

Company itself or by authorized service providers. Only anonymized usage data is used to improve the services.

(2) The undertaking of the contractually agreed Processing of Data shall be carried out essentially within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled. In these cases, the appropriate level of protection is determined by an adequacy decision by the European Commission or on the basis of special guarantees, such as contractual obligations through so-called Standard Data Protection Clauses of the Commission, the existence of certifications or binding internal data protection regulations.

**2.1.2 Sharing data between users**

(1) Collaboration in Conceptboard takes place within interactive workspaces (the "boards"). Users can transfer data to these boards. Once the user shares a board with other users, also some of this data (e.g. users' names, their profile pictures, the content they contributed, information about when they contributed) is also shared to enable the collaboration.

(2) The Supplier has no influence on data sharing between users.

**2.2 Type of Data**

(1) The Subject Matter of the processing of personal data comprises the following data types/categories:

- Personal Master and Contact Data (e.g. name, email, contact details, profile picture)

- Personenstamm- und Kontaktdaten (z.B. Name, Email, Kontaktdetails, Profilbild)
- Inhaltsdaten (z.B. Texteingaben, Support-Anfragen)
- Kundenhistorie und Nutzungsverhaltensdaten (z.B. Änderungshistorie an Inhalten)
- Identifikations- und Authentifizierungsdaten (z.B. IP-Adresse, User-ID, Session-Cookie, Login-Token)
- Inhaltsdaten auf den interaktiven Arbeitsbereichen („Boards"), diese können je nach Nutzung auch personenbezogene Daten enthalten

(2) Bitte beachten Sie, dass der SaaS-Dienst Conceptboard nicht für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 und Art. 10 DS-GVO geeignet ist.

### 2.3 Kategorien betroffener Personen

(1) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Nutzer

(2) Gegebenenfalls können sich in den Inhaltsdaten der jeweiligen Boards im Rahmen der Nutzerzusammenarbeit auch personenbezogene Daten von anderen Betroffenen befinden. Auf diese Art der Nutzung hat der Auftragnehmer keinen Einfluss und demzufolge auch keine Kenntnis darüber, welche Betroffenen es konkret sind.

## 3 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor

- Content Data (e.g. text input, support requests)
- Customer History and Usage Behavior (e.g. modification history on content)
- Identification and Authentication Data (e.g. IP address, user ID, session cookie, login tokens)
- Content Data within the interactive workspaces (the "boards"), which, depending on the actual use, can include personal data

(2) Please note that the SaaS service Conceptboard has not been designed for the processing of special categories of personal data as defined in Article 9 and Article 10 GDPR.

### 2.3 Categories of Data Subjects

(1) The Categories of Data Subjects comprise:

- Users

(2) As the case may be, personal data of other data subjects may also be found in the content data of the interactive workspaces ("boards") in the context of user collaboration. The Supplier has no influence on this type of use and therefore also no knowledge of which persons are affected.

## 3 Technical and Organizational Measures

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organizational Measures, set out in advance of the

Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (Einzelheiten in „Anhang 1: TOM").

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mindestens in Textform mitzuteilen.

(4) Bitte beachten Sie, dass der SaaS-Dienst Conceptboard nicht für die Verarbeitung besonderer Kategorien

awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account (details in "Appendix 1: TOM").

(3) The Technical and Organizational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented and communicated to the Client at least in text form.

(4) Please note that the SaaS service Conceptboard has not been designed for the processing of special categories of personal data as defined in Article 9 and Article 10 GDPR.

personenbezogener Daten im Sinne des Art. 9 und Art. 10 DS-GVO geeignet ist.

## 4 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft sind nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer verpflichtet sich, bei der

## 4 Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

(2) Erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay. For such assistance, the contractor may claim a fee.

## 5 Quality assurance and other duties of the Supplier

(1) In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

a) Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR. His/Her current contact details are always available and easily accessible on the website of the Supplier.

b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier undertakes to

auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertragsverhältnisses mit dem Auftraggeber fort. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung des Beschäftigungsverhältnisses fort. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in "Anhang 1: TOM").

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten

maintain confidentiality when processing the Client's personal data in accordance with the order. This continues even after the contractual relationship with the client has ended. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The confidentiality obligation continues to exist even after the employment relationship has ended. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

c) Implementation of and compliance with all Technical and Organizational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR (details in "Appendix 1: TOM").

d) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection

bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrags.

## 6 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von

with the processing of this Order or Contract.

f) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Cli- ent.

g) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

h) Verifiability of the Technical and Organizational Measures conducted by the Client as part of the Client's supervisory powers referred to in item 7 of this contract.

## 6 Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged

Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der in "Anhang 2: Unterauftragnehmer" genannten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Supplier may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Client. The Client agrees to the commissioning of the subcontractors named in "Appendix 2: Subcontractors" on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(5) Further outsourcing by the subcontractor requires the express consent of the main Client (at the minimum in text form); all contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

## 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Für die Ermöglichung von Kontrollen durch den Auftraggeber, kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

(4) Das Ergebnis der Kontrollen ist durch den Auftraggeber zu dokumentieren.

## 8 Mitteilungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die

## 7 Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) The Supplier may claim remuneration for enabling Client inspections.

(4) The result of the inspections must be documented by the client.

## 8 Communication obligations of the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes

Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

## 9 Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Die Weisungsentgegennahme erfolgt über den Kunden-Support des Auftragnehmers, vorzugsweise per E-Mail an support@conceptboard.com.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die

of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a personal data breach immediately to the Client.

c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.

d) Supporting the Client with its data protection impact assessment.

e) Supporting the Client with regard to prior consultation of the supervisory authority.

(2) The Supplier may claim compensation for support services which are not in- cluded in the description of the services and which are not attributable to failures on the part of the Supplier.

## 9 Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The receiving of the instructions takes place via the customer support of the Supplier, preferably by e-mail to support@conceptboard.com.

(3) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations.

Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 10 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind:

a) Kopien oder Duplikate, die im Rahmen der Nutzerzusammenarbeit temporär erforderlich sind,

b) Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind,

c) Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrags – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gegebenenfalls können Inhaltsdaten im Rahmen der Nutzerzusammenarbeit hiervon ausgenommen sein. Dies richtet sich nach dem besitzenden Nutzer ("Owner") des interaktiven Arbeitsbereichs („Board“):

a) Boards können von deren Besitzer gelöscht werden; die Löschung des Boards löst die Löschung der Inhaltsdaten aus

The Supplier is entitled to suspend the implementation of the specific instruction until it is confirmed or changed by the Client.

## 10 Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of:

a) copies or duplicates as far as they are temporarily necessary in the context of user collaboration,

b) back-up copies as far as they are necessary to ensure orderly data processing,

c) data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Main Contract, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. As the case may be, exceptions to this rule can apply to content data in the context of user collaboration. This depends on the owning user ("Owner") of the interactive workspace („Board“):

a) Boards can be deleted by their owners; the deletion of the board triggers the deletion of the content data

b) Boards that are only accessible to the owning user are deleted when the user is deleted

c) Boards that are accessible to other users but not users within the organization of the owning user ("Team Members") are deleted when the user is deleted

b) Boards, die nur dem besitzenden Nutzer zugänglich sind, werden beim Löschen des Nutzers gelöscht

c) Boards, die weiteren Nutzern, jedoch nicht Nutzern innerhalb der Organisation des besitzenden Nutzers ("Team Members"), zugänglich sind, werden beim Löschen des Nutzers gelöscht

d) Boards, die weiteren Nutzern innerhalb der Organisation des besitzenden Nutzers ("Team Members") zugänglich sind, gehen beim Löschen des Nutzers in das Besitztum eines dieser weiteren Nutzer über

e) Inhaltsdaten eines Nutzers, die nach der Löschung des Nutzers auf anderen Boards bestehen bleiben (z.B. Kommentare), werden als von einem "gelöschten Nutzer" verursacht dargestellt

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

## 11 Haftung

(1) Auf Artikel 82 DS-GVO wird verwiesen.

## 12 Außerordentliches Kündigungsrecht

(1) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

d) Boards that are accessible to other users within the organization of the owning user ("Team Members") will, upon deletion of the user, become the property of one of these other users

e) A user's content data that persists on other boards after deleting the user (e.g., comments) is represented as being caused by a "deleted user"

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

## 11 Liability

(1) Reference is made to Article 82 GDPR.

## 12 Extraordinary right of termination

(1) The Client can terminate the contract at any time without observing a notice pe- riod if the Supplier has seriously violated data protection regulations or the provi- sions of this contract, the Supplier cannot or does not want to carry out an instruc- tion from the Client, or the Supplier re- fuses control rights by the Client contrary to the contract. In particular, non-compli- ance with the obligations stipulated in this

Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

contract and derived from Article 28 GDPR constitutes a serious violation.

UNTERSCHRIFTENSEITE
*SIGNATURE PAGE*

| **Auftraggeber**<br>***Client*** | **Auftragnehmer**<br>***Supplier*** |
|---|---|
| Petra Banik | Helmut Schmitz |
| Name<br>*Name* | Name<br>*Name* |
| Leitung Rechtsstelle | Geschäftsführer / CEO |
| Position<br>*Position* | Position<br>*Position* |
| 2.3.2021 | 2. März 2021 |
| Datum<br>*Date* | Datum<br>*Date* |
| i.V. | |
| Signatur<br>*Signature* | Signatur<br>*Signature* |

ANHANG 1: TOM
*APPENDIX 1: TOM*

**Präambel**
Wir – die Conceptboard Cloud Service GmbH, Mansfelder Str. 56, 06108 Halle (Saale), Deutschland – treffen bei der Erbringung der Dienste gemäß Hauptvertrag zusammen mit dem Kunden – nachstehend „Auftraggeber" – unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen die folgenden technischen und organisatorischen Maßnahmen (TOM), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
Die Auswahl der Maßnahmen gliedert sich in die Bereiche:

- Pseudonymisierung
- Verschlüsselung
- Vertraulichkeit und Integrität
- Verfügbarkeit und Belastbarkeit
- Wirksamkeitsprüfung

**Preamble**
When performing the services in accordance with the main contract, we – the Conceptboard Cloud Service GmbH, Mansfelder Str. 56, 06108 Halle (Saale), Germany – meet with the customer – hereinafter referred to as the "client" – taking into account the state of the art, the implementation costs and the type, scope, circumstances and purposes of the processing, as well as the different probability and severity of the risk for the rights and freedoms of natural persons, the following technical and organizational measures (TOM) to ensure a level of protection appropriate to the risk.
The selection of measures is divided into the following areas:

- Pseudonymization
- Encryption
- Confidentiality and Integrity
- Availability and Resilience
- Effectiveness Test

**Pseudonymisierung**
Maßnahmen zur Pseudonymisierung haben den Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

1) Die Ablage und Zusammenführung personenbezogener Daten erfolgen anhand einer pseudonymisierten Nutzeridentifikationsnummer (User-ID).

**Pseudonymization**
Measures for pseudonymization have the purpose of excluding or significantly complicating the determination of the person concerned.

1) Personal data is stored and merged using a pseudonymized user identification number (user ID).

**Verschlüsselung**
Maßnahmen zur Verschlüsselung haben den Zweck die Nutzung und den Missbrauch der

**Encryption**
Encryption measures have the purpose of preventing the use and misuse of the data by

Daten durch unberechtigte Dritte – mangels Schlüssel – zu verhindern.

1) Die Kommunikation zwischen Servern und verbundenen Clients wird durchgehend unter Verwendung aktueller Technologien und akzeptierter Industriestandards verschlüsselt. Abhängig vom Client des Nutzers werden TLS1.2, 256-bit AES in GCM mit elliptischer Kurven-Kryptographie und Forward-Secrecy verwendet. Weitere Informationen zur Übertragungssicherheit finden Sie im Qualys SSL Report für Conceptboard[2].
2) Gespeicherte Daten des Kunden werden mit symmetrischen AES256-Schlüsseln verschlüsselt.
3) Nutzer-Passwörter werden nicht gespeichert. Stattdessen wird ein sicheres, auf kryptographischen Hashfunktionen basiertes Verfahren verwendet ("Salted Cryptographic Hash").

unauthorized third parties – in the absence of a key.

1) Communication between servers and connected clients is continuously encrypted using the latest technologies and accepted industry standards. Depending on the client of the user, TLS1.2, 256-bit AES in GCM with elliptic curve cryptography and forward secrecy are used. For more information on transmission security, see the Qualys SSL Report for Conceptboard[2].
2) Stored customer data is encrypted with symmetrical AES256 keys.
3) User passwords are not saved. Instead, a secure method based on cryptographic hash functions is used ("Salted Cryptographic Hash").

**Vertraulichkeit und Integrität**

Maßnahmen zur Vertraulichkeit und Integrität dienen dem Schutz personenbezogener Daten vor unbefugter Preisgabe, sowie der Sicherstellung, dass die Systeme korrekt funktionieren, und die Daten unversehrt, das heißt vollständig und durch äußere Einflüsse unverändert, bleiben.

1) Die genutzten Rechenzentren – sofern nicht anders vereinbart oder anderweitig dokumentiert die Rechenzentren der Amazon Web Services (AWS) in der Region Frankfurt, Deutschland – verfügen über umfangreiche und moderne Zutrittskontrollen (bspw. elektronische Zutrittskontrollsysteme, Kameraüberwachung, Einbruchmeldeanlagen, Wachpersonal) und implementieren Prozesse, die nachhaltig vor unbefugtem Zutritt schützen (bspw. festgelegte Sicherheitsbereiche, individuelle Zutrittsberechtigungsvergabe, rollenbasiertes Berechtigungskonzept). Weitere Informationen über die getroffenen

**Confidentiality and Integrity**

Confidentiality and integrity measures serve to protect personal data from unauthorized disclosure, as well as to ensure that the systems function correctly and the data remains intact, i.e. complete and unchanged by external influences.

1) The data centers used – unless otherwise agreed or otherwise documented the data centers of Amazon Web Services (AWS) in the Frankfurt, Germany region – have extensive and modern access controls (e.g. electronic access control systems, camera surveillance, intrusion detection systems, security guards) and implement processes that protect sustainably against unauthorized access (e.g. defined security areas, individual access authorization, role-based authorization concept). More information about the protective measures taken can be

[2] https://www.ssllabs.com/ssltest/analyze.html?d=app.conceptboard.com

Schutzmaßnahmen finden Sie im AWS Portal zur Cloud-Sicherheit[3].

2) Die genutzten Büroräume verfügen über elektronische Zutrittskontrollsysteme und Kameraüberwachung der Eingangsbereiche. Es sind Prozesse zur individuellen Zutrittsberechtigungsvergabe, der Dokumentationen von Zutrittsberechtigungen, sowie Besucher-Regulierungen implementiert. Die Büroräume sind außerhalb der Arbeitszeiten verschlossen.

3) Die öffentlich bereitgestellten Server-Systeme, die dedizierten Enterprise-Systeme je Mandant und die Entwicklungssysteme, sowie deren jeweiligen Datenspeicher- und Backup-Speicherorte, sind durch separate Netzwerke und Netzwerk-Segmente vollständig voneinander getrennt. Netzwerke und Netzwerk-Segmente sind durch restriktive Firewall-Regeln geschützt. Systemkomponenten sind entsprechend allgemein etablierter und akzeptierter Industriestandards verstärkt (bspw. Sperrung von nicht erforderlichen Ports, regelmäßige Software-Updates).

4) Administrativer Zugang erfolgt nur über sichere Verbindungen (VPN mit Ende-zu-Ende-Verschlüsselung, separate Management-Netzwerke, Jump-Hosts, 2FA) und wird in Log-Files protokolliert. Zugänge zur Administration und zur Wartung sind eindeutig natürlichen Personen zugeordnet.

5) Die Vergabe von Zugriffsrechten erfolgt unter Einhaltung spezifischer Genehmigungsregelungen und wird dokumentiert. Das Prinzip der geringsten Rechtevergabe ("Need-to-Know-Prinzip"), nachdem Nutzer nur diejenigen Zugänge erhalten, die für die Erfüllung ihrer Aufgaben nötig sind, wird eingesetzt. Zugriffsrechte für IT-Systeme werden regelmäßig überprüft und entzogen, sobald die geschäftliche Notwendigkeit für den Zugriff nicht mehr besteht. Kritische administrative

found on the AWS Portal for Cloud Security[3].

2) The offices used have electronic access control systems and camera surveillance of the entrance areas. Processes for individual access authorization, documentation of access authorizations and visitor regulations have been implemented. The offices are locked outside of working hours.

3) The publicly provided server systems, the dedicated enterprise systems per client and the development systems, as well as their respective data storage and backup storage locations, are completely separated from each other by separate networks and network segments. Networks and network segments are protected by restrictive firewall rules. System components are reinforced in accordance with generally established and accepted industry standards (e.g. blocking unnecessary ports, regular software updates).

4) Administrative access is only possible via secure connections (VPN with end-to-end encryption, separate management networks, jump hosts, 2FA) and is logged in log files. Access to administration and maintenance are clearly assigned to natural persons.

5) The granting of access rights takes place in compliance with specific approval regulations and is documented. The principle of the lowest allocation of rights ("need-to-know principle"), after users only receive the access that is necessary for the fulfillment of their tasks, is used. Access rights to IT systems are regularly checked and withdrawn as soon as the business need for access no longer exists. Critical administrative combinations of rights are monitored ("separation-of-duty principle").

6) All employees are familiar with the handling of confidential data and are obliged in writing to maintain confidentiality. There

[3] https://aws.amazon.com/security/

Rechtekombinationen werden überwacht ("Separation-of-Duty-Prinzip").

6) Alle Mitarbeiter sind im Umgang mit vertraulichen Daten unterrichtet und schriftlich auf die Wahrung der Vertraulichkeit verpflichtet. Verbindliche Regeln für die Einsichtnahme in und die Offenlegung von sensiblen Daten, sowie schriftliche Richtlinien für die Übertragung und Weitergabe von Daten bestehen. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers.
7) Arbeitsgeräte sind mit Sicherheitssoftware wie bspw. Firewalls, Antivirus-Software und Malware-Erkennung ausgestattet. Schriftliche Regelungen zum Umgang mit mobilen Geräten und Datenträgern, zur sicheren Datenlöschung, zur Vernichtung von Datenträgern, sowie zur Remote-Arbeit (Home-Office) bestehen. Unbeaufsichtigte IT-System werden automatisch gesperrt.
8) Passwörter erfordern eine definierte Mindestkomplexität. Initiale Passwörter müssen nach der ersten Anmeldung geändert werden.

are binding rules for inspecting and disclosing sensitive data, as well as written guidelines for the transfer and transmission of data. The processing of personal data takes place exclusively in accordance with the instructions of the client.
7) Work devices are equipped with security software such as firewalls, antivirus software and malware detection. Written regulations exist for handling mobile devices and data carriers, for secure data deletion, for the destruction of data carriers, and for remote work (home office). Unattended IT systems are automatically blocked.
8) Passwords require a defined minimum complexity. Initial passwords must be changed after the first login.

**Verfügbarkeit und Belastbarkeit**

Die Maßnahmen zur Verfügbarkeit und Belastbarkeit haben den Zweck, die Dienste und internen Betriebsabläufe, sowie deren Informationssicherheit, auch bei Betriebsstörungen und unvorhergesehenen Ereignissen zu gewährleisten.

1) Die genutzten Rechenzentren – sofern nicht anders vereinbart oder anderweitig dokumentiert die Rechenzentren der Amazon Web Services (AWS) in der Region Frankfurt, Deutschland – verfügen über umfangreiche und moderne Brandmelde- und Löscheinrichtungen, Klima- und Temperaturregelungen, sowie Maßnahmen zum Überspannungsschutz und zur unterbrechungsfreien

**Availability and Resilience**

The measures for availability and resilience have the purpose of guaranteeing the services and internal operational processes, as well as their information security, even in the event of operational disruptions and unforeseen events.

1) The data centers used – unless otherwise agreed or otherwise documented the data centers of Amazon Web Services (AWS) in the Frankfurt, Germany region – have extensive and modern fire alarm and extinguishing devices, climate and temperature controls, as well as measures for surge protection and uninterruptible power supply (UPS). For more information, see the AWS Cloud Security Portal[4].

Stromversorgung (USV). Weitere Informationen finden Sie im AWS Portal zur Cloud-Sicherheit[4].

2) Die Inbetriebnahme der bereitgestellten Produktiv-Systeme, deren Konfiguration und das Einspielen von Änderungen erfolgen nachvollziehbar und transparent über eine automatisierte Deployment-Infrastruktur ("Infrastructure-as-Code-Prinzip").
3) Backups der Produktiv-Daten erfolgen stündlich in inkrementeller Form und täglich als Voll-Backup. Alle Backups werden redundant und in verschlüsselter Form (AES256) über mehrere Geräte und mindestens 3 getrennte Einrichtungen – sofern nicht anders vereinbart oder anderweitig dokumentiert innerhalb der Rechenzentren der Amazon Web Services (AWS) in der Region Frankfurt, Deutschland – verteilt vorgehalten. Technische Zugriffsbeschränkungen, automatische Historisierungs- und Lösch-Policies, sowie strikte organisatorische Vorgaben zum Umgang mit Backups sind implementiert.
4) Disaster-Recovery-Prozesse für die Datenwiederherstellung und Prozesse zur stichprobenartigen Prüfung der Wiederherstellungsfähigkeit sind definiert.
5) Capacity-Management-Maßnahmen zur Überwachung des Resourcen-Verbrauchs der Systeme sowie der Planung des zukünftigen Ressourcen-Bedarfs sind implementiert.
6) Verfahren zum Umgang und der Meldung von Störungen (Incident-Management) inklusive der Erkennung und Reaktion auf mögliche Sicherheitsvorfälle sind definiert.

**Wirksamkeitsprüfung**
Die Maßnahmen zur Wirksamkeitsprüfung dienen der regelmäßigen Kontrolle und Bewertung der Effektivität aller zuvor beschriebenen technischen und organisatorischen Maßnahmen.

2) The commissioning of the productive systems provided, their configuration and the import of changes are carried out traceably and transparently via an automated deployment infrastructure ("infrastructure-as-code principle").
3) Productive data is backed up hourly in incremental form and daily as a full backup. All backups are kept redundant and in encrypted form (AES256) over several devices and at least 3 separate facilities – unless otherwise agreed or otherwise documented within the data centers of Amazon Web Services (AWS) in the Frankfurt, Germany region. Technical access restrictions, automatic historization and deletion policies, as well as strict organizational requirements for handling backups are implemented.
4) Disaster recovery processes to restore data and processes for randomly checking the recoverability are defined.
5) Capacity management measures to monitor the resource consumption of the systems as well as the planning of future resource requirements are implemented.
6) Procedures for handling and reporting incidents (incident management) including the detection and reaction to possible security incidents are defined.

**Effectiveness Test**
The measures for effectiveness testing serve to regularly check and evaluate the effectiveness of all the technical and organizational measures described above.

[4] https://aws.amazon.com/security/

1) Datenschutzkoordinatoren sind definiert und beauftragt Änderungen in den internen Arbeitsprozessen aus Datenschutzsicht zu begleiten, auf Datenschutzaspekte hinzuweisen, und mit dem Datenschutzbeauftragten abzustimmen. Mitarbeiter sind angewiesen erkannte Verletzungen der Datenschutzbestimmungen, Verdacht auf mögliche Verletzungen, sowie sonstige Vorfälle mit Bezug zur Informationssicherheit umgehend den Datenschutzkoordinatoren zu melden. Disziplinarmaßnahmen bei Zuwiderhandlung gegen Geheimhaltungsverpflichtungen bestehen.

2) Regelmäßige Besprechungen des Datenschutzbeauftragten mit den Datenschutzkoordinatoren inklusive der Überprüfung der Betriebsprozesse, welche die Verarbeitung von personenbezogenen Daten betreffen, und der Revision der zugehörigen technischen und organisatorischen Maßnahmen finden statt.

3) Sicherheitsprüfungen (bspw. Penetrationstests) durch externe Parteien sind nach Absprache möglich und werden aktiv unterstützt. IT-Sicherheitsforscher, welche valide Sicherheitsrisiken identifizieren, werden öffentlich in Conceptboard's Security Hall of Fame genannt.

1) Data protection coordinators are defined and commissioned to accompany changes in internal work processes from a data protection perspective, to point out data protection aspects and to coordinate with the data protection officer. Employees are instructed to immediately report any identified violations of data protection regulations, suspected possible violations, or other incidents related to information security to the data protection coordinators. Disciplinary measures exist in the event of non-compliance with confidentiality obligations.

2) There are regular meetings between the data protection officer and the data protection coordinators, including the review of the operating processes that affect the processing of personal data and the revision of the associated technical and organizational measures.

3) Security checks (e.g. penetration tests) by external parties are possible after consultation and are actively supported. IT security researchers who identify valid security risks are publicly mentioned in Conceptboard's Security Hall of Fame.

## ANHANG 2: UNTERAUFTRAGNEHMER
## *APPENDIX 2: SUBCONTRACTORS*

| Service | Address | Purpose | Exchanged Personal Data |
|---|---|---|---|
| AWS | Amazon Web Services EMEA SARL<br>38 Avenue John F. Kennedy<br>L-1855, Luxembourg | Data Center & Virtual Server Operation | – IP address<br>– User content (continuously encrypted*) |
| Host Europe | Host Europe GmbH<br>Hansestrasse 111<br>51149 Köln, Germany | Email Server Hosting | – User email address<br>– Email content |
| SendinBlue | SendinBlue SAS 47<br>Rue de la Chaussée d'Antin<br>75009 Paris, France | Onboarding, Product Update Emails | – User email address<br>– User name |

*** Nutzerinhalte werden durchgehen verschlüsselt übertragen und gespeichert, und lediglich durch Conceptboard-interne Komponenten innerhalb der virtuellen Server in entschlüsselter Form verarbeitet.**

**** User content is transmitted and stored in encrypted form and only processed in decrypted form by Conceptboard-internal components within the virtual servers.***

**Optional:**

**Der Auftraggeber hat die Möglichkeit, die von folgenden Unterauftragnehmern angebotenen Zusatzfunktionen zu deaktivieren, und damit jegliche zugehörige Datenübermittlung zu unterbinden.**

***The Client has the option of deactivating the additional functions offered by the following subcontractors and thus preventing any associated data transmission.***

| Service | Address | Purpose | Exchanged Personal Data |
|---|---|---|---|
| Zendesk | Zendesk, Inc.<br>1019 Market Street<br>San Francisco, CA 94103, USA | Support Ticket Management & Help Center Hosting | – User email address<br>– User name<br>– IP address<br>– Cookie data<br>– Support content |
| Tokbox | Vonage Holdings Corp.<br>23 Main Street<br>Holmdel, NJ 07733, USA | In-App Video Conferencing | – IP address<br>– Cookie data<br>– Audio/video stream |
| Aspose | Aspose Pty Ltd.<br>79 Longueville Road, Suite 163<br>Lane Cove, NSW, 2066, Australia | Office File Conversion (Word, Powerpoint, Excel) | – Upload content |