# Auftragsverarbeitungsvertrag (AVV)

## Data Processing Agreement (DPA)

**1. Präambel**

Die aufinity Group GmbH (nachfolgend "Auftragsverarbeiter") verarbeitet für den Kunden (nachfolgend "Verantwortlicher") im Auftrag und in Erfüllung ihrer vertraglichen Verpflichtungen gemäß ihrer Allgemeinen Geschäftsbedingungen sowie der jeweils abgeschlossenen Auftragsformulare (nachfolgend "Hauptvertrag") personenbezogene Daten nach Art. 28 der Datenschutz-Grundverordnung (nachfolgend "DSGVO"). Dieser Auftragsverarbeitungsvertrag (nachfolgend "AVV") konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die mit dem Hauptvertrag in Verbindung stehen.

**1. Preamble**

The aufinity Group GmbH (hereinafter "Processor") processes personal data on behalf of the Client (hereinafter "Controller") in accordance with Art. 28 of the General Data Protection Regulation (hereinafter "GDPR") and in fulfillment of its contractual obligations in accordance with its General Terms and Conditions and the respective Order Forms concluded (hereinafter together "Main Agreement"). This Data Processing Agreement (hereinafter "DPA") specifies the data protection obligations of the Parties in connection with the Main Agreement.

**2. Umfang der Verarbeitung**

2.1. Gegenstand und Dauer, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten, sowie die Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

2.2. Die Laufzeit dieses AVV richtet sich nach der Laufzeit des Hauptvertrags. Das Recht zur außerordentlichen Kündigung bleibt hiervon unberührt.

**2. Scope of the Processing**

2.1 The subject matter and duration, nature and purposes of the processing, the type of personal data and the categories of data subjects are set out in **Annex 1**.

2.2. The term of this DPA is based on the term of the Main Agreement. The right to extraordinary termination remains unaffected by this.

**3. Weisungsbefugnis**

3.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich weisungsgebunden im Rahmen der Anordnungen des Verantwortlichen. Die Weisungen werden durch diese AVV festgelegt und können von dem Verantwortlichen durch einzelne Weisungen in Textform geändert, ergänzt oder ersetzt werden. Die vom Verantwortlichen erteilten Weisungen sind sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter zu dokumentieren.

3.2. Erteilt der Verantwortliche Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten von dem Verantwortlichen zu tragen, sofern diese

**3. Instruction Authority**

3.1. The Processor processes personal data exclusively in accordance with the instructions of the Controller. The instructions are set out in this DPA and may be amended, supplemented or replaced by the Controller by means of individual instructions in text form. The instructions issued by the Controller must be documented by both the Controller and the Processor.

3.2. If the Controller issues individual instructions that go beyond the contractually agreed scope of services, the resulting costs shall be borne by the Controller, unless they are necessary to prevent or remedy legal

nicht erforderlich sind, um Rechtsverstöße im Zuständigkeitsbereich des Auftragsverarbeiters zu verhindern bzw. abzustellen.

violations in the Processor's area of responsibility.

3.3. Sofern der Auftragsverarbeiter durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, dazu verpflichtet ist, personenbezogene Daten außerhalb der Weisungen des Verantwortlichen zu verarbeiten, teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Im letztgenannten Fall wird der Auftragsverarbeiter den Verantwortlichen unverzüglich informieren, sobald dies rechtlich möglich ist.

3.3. Where the Processor is required by Union or Member State law to which the Processor is subject to process personal data outside the instructions of the Controller, the Processor shall notify the Controller of such legal requirements before processing, unless the law in question prohibits such notification on grounds of important public interest. In the latter case, the Processor will inform the Controller without undue delay as soon as legally possible.

3.4. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragsverarbeiter darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Verantwortlichen bestätigt oder abgeändert wurde.

3.4. The Processor shall inform the Controller without undue delay if it considers that an instruction violates applicable laws. The Processor may suspend the implementation of the Instruction until it has been confirmed or amended by the Controller.

**4. Vertraulichkeit**

Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

**4. Confidentiality**

The Processor guarantees that the individuals authorized to process personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.

**5. Technische und Organisatorische Maßnahmen**

5.1. Der Auftragsverarbeiter trifft alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten des Verantwortlichen. Die Parteien vereinbaren dazu die in **Anlage 2** zu diesem AVV niedergelegten konkreten technischen und organisatorischen Maßnahmen.

**5. Technical and organizational measures**

5.1. The Processor shall ensure all technical and organizational measures required under Art. 32 GDPR to protect the Controller's data. To this end, the Parties agree on the specific technical and organizational measures set out in **Annex 2** to this DPA.

5.2. Zur Anpassung an technische und rechtliche Gegebenheiten ist es dem Auftragsverarbeiter gestattet, die getroffenen Maßnahmen insoweit zu ändern. Dabei darf das vertraglich vereinbarte Sicherheitsniveau nicht unterschritten werden.

5.2. In order to adapt to technical and legal circumstances, the Processor is permitted to change the measures taken in this respect. In doing so, the contractually agreed security level shall not be undercut.

**6. Betroffenenrechte**

6.1. Für die Wahrung von Betroffenenrechten ist allein der Verantwortliche verantwortlich.

6.2. Der Auftragsverarbeiter wird angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in der DSGVO genannten Rechte der betroffenen Person nachzukommen.

6.3. Der Auftragsverarbeiter ist nur nach vorheriger Zustimmung durch den Verantwortlichen befugt, Auskünfte an Dritte oder Betroffene zu erteilen. Entsprechende Anfragen leitet der Auftragsverarbeiter unverzüglich an den Verantwortlichen weiter.

**6. Data Subject Rights**

6.1. The Controller is solely responsible for safeguarding the rights of data subjects.

6.2. Given the nature of the processing, the Processor will, where possible, support the Controller with appropriate technical and organizational measures to comply with its obligation to respond to requests to exercise the rights of the data subject referred to in the GDPR.

6.3. The Processor is only authorized to provide information to third parties or data subjects with the prior consent of the Controller. The Processor shall immediately forward such requests to the Controller.

**7. Unterstützungspflicht**

7.1. Unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen wird der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten unterstützen.

7.2. Der Auftragsverarbeiter unterrichtet den Verantwortlichen, wenn er in Bezug auf die Verarbeitung eine schwerwiegende Störung des Betriebs oder einen Verstoß gegen diese Vereinbarung oder gegen datenschutzrechtliche Vorschriften beim Auftragsverarbeiter feststellt.

**7. Support obligation**

7.1. Taking into account the nature of the processing and the information available, the Processor shall assist the Controller in complying with the obligations set out in Art. 32-36 GDPR.

7.2. The Processor shall inform the Controller if it becomes aware of a serious disruption to the Processor's operations or a breach of this DPA or of data protection regulations in relation to the processing.

**8. Löschung oder Rückgabe**

Nach Abschluss der Erbringung der Verarbeitungsleistungen wird der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen oder zurückgeben und die vorhandenen Kopien löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

**8. Deletion or Return**

After completion of the provision of services relating to processing, the Processor will either delete or return all personal data at the discretion of the Controller and delete the existing copies, unless there is an obligation to store the personal data under Union or Member State law.

**9. Kontrollrechte**

9.1. Der Auftragsverarbeiter wird dem Verantwortlichen auf Verlangen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung stellen und Überprüfungen – einschließlich Inspektionen –, die

**9. Control Rights**

9.1. Upon request, the Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out in Art. 28 GDPR and shall enable and contribute to audits - including inspections - carried out by the Controller

vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen.

or another auditor commissioned by the Controller.

9.2. Den mit einer Inspektion betrauten Personen ist von dem Auftragsverarbeiter soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragsverarbeiter ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Inspektion erforderlich sind.

9.2. The individuals entrusted with an inspection must be granted access and insight by the Processor as far as necessary. The Processor is obliged to provide the necessary information, demonstrate procedures and provide the evidence required to carry out an inspection.

9.3. Inspektionen haben ohne vermeidbare Störungen des Geschäftsbetriebs des Auftragsverarbeiters zu erfolgen. Soweit nicht aus vom Verantwortlichen zu dokumentierenden, dringenden Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragsverarbeiters, sowie nicht häufiger als alle 12 Monate statt.

9.3. Inspections must be carried out without avoidable disruption to the Processor's business operations. Unless otherwise indicated for urgent reasons to be documented by the Controller, inspections shall take place after reasonable advance notice and during Processor's business hours, and not more frequently than every 12 months.

9.4. Der Verantwortliche trägt die Kosten der für die Erfüllung der Kontrollrechte erforderlichen Maßnahmen, mit Ausnahme von Maßnahmen, die wegen eines Gesetzes- oder Vertragsverstoßes durch den Auftragsverarbeiters erforderlich wurden.

9.4. The Controller shall bear the costs of the measures necessary for the fulfillment of the inspection rights, with the exception of measures required due to a breach of law or contract by the Processor.

**10. Ort der Datenverarbeitung**

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet in einem Mitgliedstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Der Verantwortliche stimmt einer Verlagerung der Verarbeitung in ein Drittland zu, sofern die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

**10. Location of Data Processing**

The provision of the contractually agreed data processing takes place in a member state of the European Union (EU) or in another state party to the Agreement on the European Economic Area (EEA). The Controller consents to the transfer of processing to a third country, provided that the requirements of Art. 44 et seq. GDPR are met.

**11. Einsatz von Unterauftragsverarbeitern**

11.1. Die Parteien legen in **Anlage 3** fest, welche Unterauftragsverarbeiter eingesetzt werden.

**11. Appointment of Subprocessors**

11.1. The Parties shall specify in **Annex 3** which subprocessors are to be used.

11.2. Der Verantwortliche genehmigt den Einsatz weiterer oder den Ersatz bestehender Unterauftragsverarbeiter. Der Auftragsverarbeiter wird den Verantwortlichen vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragnehmers informieren.

11.2. The Controller shall authorize the use of additional or the replacement of existing subprocessors. The Processor shall inform the Controller in advance of any intended change regarding the use or replacement of a subprocessor.

11.3. Der Verantwortliche kann gegen eine

11.3. The Controller may object to an intended change.

beabsichtigte Änderung Einspruch erheben. Erhebt der Verantwortliche Einspruch, wird der Auftragsverarbeiter bis zur Klärung des Einspruchs davon absehen, den jeweiligen Unterauftragnehmer einzusetzen. Erfolgt innerhalb von 14 Tagen nach Information keine Antwort des Verantwortlichen, gilt die Änderung als bestätigt.

If the Controller raises an objection, the Processor shall refrain from using the respective subcontractor until the objection has been clarified. If there is no response from the responsible party within 14 days of being informed, the change shall be deemed confirmed.

11.4. Der Auftragsverarbeiter hat ein außerordentliches Kündigungsrecht, wenn sich der Verantwortliche nach Ansicht des Auftragsverarbeiters ohne triftigen Grund weigert, den Unterauftragsverarbeiter zu genehmigen, oder wenn es dem Auftragsverarbeiter nicht möglich ist, seine Dienstleistungen ohne den abgelehnten Unterauftragsverarbeiter zu erbringen.

11.4. The Processor shall have an extraordinary right of termination if, in the Processor's opinion, the Controller refuses to involve the subprocessor without good reason, or if it is not possible for the Processor to provide the service without the rejected subprocessor.

11.5. Bei Einschaltung eines Unterauftragsverarbeiters werden diesem durch den Auftragsverarbeiter dieselben Datenschutzpflichten auferlegt, die in der AVV festgelegt sind.

11.5. If a subprocessor is engaged, the Processor shall impose the same data protection obligations on the subprocessor as set out in the DPA.

**12. Schlussbestimmungen**

12.1. Bei Auslegungsfragen und Streitigkeiten gilt ausschließlich der deutsche Text.

12.2. Im Übrigen finden die Allgemeinen Geschäftsbedingungen[1] des Auftragsverarbeiters Anwendung.

**12. Final Provisions**

12.1. In case of questions of interpretation and disputes, the German text shall apply exclusively.

12.2. In all other respects, the General Terms and Conditions[1] of the Processor shall apply.

[1] https://www.bezahl.de/agb.

# Anlage 1: Beschreibung der Verarbeitung

## Annex 1: Description of the Processing

| | |
|---|---|
| **Gegenstand der Verarbeitung**<br>*Subject-Matter of the Processing* | Unterstützung des Rechnungswesens und der Buchhaltung des Verantwortlichen durch die Zuordnung und Verbuchung von Zahlungen seiner Endkunden mittels des Versands von Zahlungseinladungen sowie der Integration von Zahlungsmethoden von Drittanbietern<br>*Supporting the accounting and bookkeeping of the Controller by allocating and reconciling payments from its end customers by means of sending payment invitations and integrating third-party payment methods* |
| **Dauer der Verarbeitung**<br>*Duration of the Processing* | Basierend auf der Laufzeit des Hauptvertrags<br>*Based on the term of the Main Agreement* |
| **Art der Verarbeitung**<br>*Nature of the Processing* | Organisation, Ordnen, Speicherung, Auslesen, Abfragen, Verwendung, Übermittlung, Abgleich, Verknüpfung<br>*Organization, structuring, storage, retrieval, consultation, use, transmission, alignment, combination* |
| **Zweck der Verarbeitung**<br>*Purpose of the Processing* | Erbringung der Dienstleistungen des Auftragsverarbeiters gemäß Hauptvertrag<br>*Provision of the Processor's services in accordance with the Main Agreement* |
| **Art der personenbezogenen Daten**<br>*Type of Personal Data* | Name, Adresse, Telefonnummer, E-Mail-Adresse und sonstige Kontaktdaten, Vertrags- und Rechnungsdaten, Transaktionsdaten (Betrag, Verwendungszweck, Bankverbindung) und sonstige leistungsrelevanten Kundendaten, Systemnutzungsdaten (IP-Adresse, Geräteangabe, Browser, Betriebssystem, Zugriffszeitpunkt)<br>*Name, address, telephone number, e-mail address and other contact data, contract and invoice data, transaction data (amount, purpose, bank details) and other performance-related customer data, system usage data (IP address, device details, browser, operating system, time of access)* |
| **Kategorien betroffener Personen**<br>*Categories of Data Subjects* | Endkunden und Mitarbeiter des Verantwortlichen<br>*End-Customers and Employees of the Controller* |

# Anlage 2: Technische und organisatorische Maßnahmen

## Annex 2: Technical and Organizational Measures

### 1. Gewährleistung der Vertraulichkeit

#### 1.1. Zugangskontrolle

Das Büro der aufinity Group GmbH verfügt über einen Schließmechanismus, eine Alarmanlage mit Videoüberwachung und eine Anbindung an einen Sicherheitsdienst. Die IT-Systeme werden in gesicherten Rechenzentren betrieben und befinden sich dort in abgeschlossenen und alarmgesicherten Serverschränken. Zutritt, Schlüssel und Nummerncodes zu den Serverschränken haben ausschließlich autorisierte und namentlich benannte Administratoren. Dritte haben nur in Begleitung von Mitarbeitern Zugang. Für den Fall einer temporären Autorisierung Dritter existieren passwortgeschützte Anmeldeprozesse. Mithilfe von Codekarten, Handscans oder PINs werden individuelle Zutrittsberechtigungen zu einzelnen Abschnitten in den Rechenzentren geregelt, sowie sämtliches Betreten und Verlassen durch die Rechenzentren-Sicherheit elektronisch protokolliert und per Videoüberwachung aufgezeichnet.

#### 1.2. Speicher- und Zugriffskontrolle

Produktivdaten werden ausschließlich von einem ausgewählten IT-Dienstleister - im Folgenden nur IT-Dienstleister genannt - bearbeitet. Ein Zugriff ist nur durch seine Administratoren möglich. Logdaten werden innerhalb des Netzes dieses IT-Dienstleisters gespeichert. Audit-Logs werden zusätzlich an einen deutschen Logprovider übertragen. Kundenservice Mitarbeiter haben eingeschränkten Zugriff auf Nutzer und Transaktionsdaten, die für die Prozesse notwendige Informationen enthalten. Informationsträger mit vertraulichen Informationen sind als vertrauliches Schriftgut zu entsorgen oder zu vernichten. Nicht mehr benötigte Datenträger sind physisch zu löschen oder zu vernichten.

#### 1.3. Datenträgerkontrolle

Der Zugriff auf die IT-Systeme ist nur mit verschlüsselten, authentifizierten Verbindungen

### 1. Guarantee of confidentiality

#### 1.1. Access control

The aufinity Group GmbH office has a locking mechanism, an alarm system with video surveillance and a connection to a security service. The IT systems are operated in secure data centers and are located in locked and alarm-protected server cabinets. Only authorized and named administrators have access, keys and number codes to the server cabinets. Third parties only have access when accompanied by employees. Password-protected login processes are in place for the temporary authorization of third parties. With the help of code cards, hand scans or PINs, individual access authorizations to individual sections of the data centers are regulated, and all entries and exits are electronically logged by data center security and recorded by video surveillance.

#### 1.2. Storage and access control

Productive data is processed exclusively by a selected IT service provider - hereinafter referred to as the IT service provider. Access is only possible by its administrators. Log data is stored within the network of this IT service provider. Audit logs are also transmitted to a German log provider. Customer service employees have limited access to users and transaction data that contain information necessary for the processes. Information carriers containing confidential information must be disposed of or destroyed as confidential documents. Data carriers that are no longer required must be physically deleted or destroyed.

#### 1.3. Data carrier control

IT system access is only possible with encrypted, authenticated connections and is logged in the access

möglich und wird im Access-Log protokolliert und nach Projektanforderung aufbewahrt. Die Storage-Systeme werden dauerhaft überwacht. Jeder ungeplante Ausfall eines Datenträgers wird sofort registriert und per E-Mail an eine Administratorgruppe gemeldet. In Problemfällen wird der RZ-Betreiber unverzüglich alarmiert und dazu aufgefordert, den betroffenen Server sofort in Augenschein zu nehmen. Nicht mehr benötigte und defekte Speichermedien werden vor dem Austausch durch den Hersteller oder einen von ihm beauftragten Dritten datenschutzgerecht gelöscht.

**1.4. Pseudonymisierung und Verschlüsselung**
Personenbezogene Daten und Datenverarbeitungsvorgänge werden im Rahmen der Möglichkeit pseudonymisiert. Gespeicherte Daten werden gelöscht, sobald sie für ihre Zweckbestimmung nicht mehr erforderlich sind und der Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen.Sind die Daten für andere und gesetzlich zulässige Zwecke erforderlich, wird deren Verarbeitung eingeschränkt.

## 2. Gewährleistung der Integrität

**2.1. Eingabekontrolle**
Alle Daten werden im Rechenzentrum des IT-Dienstleisters verarbeitet. Zusätzlich werden über sogenannte Audit-Logs die Kerndaten parallel in einem internen und externen System gespeichert.

**2.2. Transportkontrolle**
Die Daten der aufinity Group GmbH werden ausschließlich in gesicherten Rechenzentren gespeichert und verarbeitet. Alle Verbindungen sind SSL-Verschlüsselt. Alle Daten, die Kundenservice erhoben und verarbeitet werden, werden über verschlüsselte Verbindungen ausgetauscht.

**2.3. Auftragskontrolle**
Die aufinity Group GmbH verpflichtet alle Personen, die personenbezogene Daten verarbeiten, das Datengeheimnis, das Telekommunikationsgeheimnis nach § 88 TKG sowie das Sozialgeheimnis nach § 35 Abs. 1 SGB I einzuhalten und sorgt für eine entsprechende Unterweisung. An Dritte erfolgt eine Übermittlung von Daten nur, wenn dies zum Zweck der Vertragsabwicklung notwendig ist oder der Kunde zuvor eingewilligt hat. Einmal jährlich wird der

log and stored according to project requirements. The storage systems are permanently monitored. Any unplanned failure of a data carrier is registered immediately and reported to an administrator group by e-mail. In the event of a problem, the data center operator is alerted immediately and requested to inspect the affected server immediately. Defective storage media that are no longer required are deleted in accordance with data protection regulations before being replaced by the manufacturer or a third party commissioned by the manufacturer.

**1.4. Pseudonymization and encryption**
Personal data and data processing operations are pseudonymized where possible. Stored data is deleted as soon as it is no longer required for its intended purpose and the deletion does not conflict with any statutory retention obligations; if the data is required for other and legally permissible purposes, its processing is restricted.

## 2. Guarantee of integrity

**2.1. Input control**
All data is processed in the IT service provider's data center. In addition, the core data is stored in parallel in an internal and external system via so-called audit logs.

**2.2. Transport control**
The data of aufinity Group GmbH is stored and processed exclusively in secure data centers.
All connections are SSL-encrypted.
All data collected and processed by customer service is exchanged via encrypted connections.

**2.3. Order control**
All persons who process personal data are obliged by aufinity group GmbH to comply with data secrecy, telecommunications secrecy in accordance with Section 88 TKG and social secrecy in accordance with Section 35 (1) SGB I and ensures that they are instructed accordingly. Data will only be transferred to third parties if this is necessary for the purpose of processing the contract or if the customer has given their prior consent. Once a year, the hosting provider is

Hosting-Anbieter auf Einhaltung der Richtlinie zum Umgang mit personenbezogenen Daten überprüft. Die Subunternehmer werden sorgfältig ausgewählt.

checked for compliance with the policy on handling personal data. Subcontractors are carefully selected.

**2.4. Trennungskontrolle**

Es erfolgt eine Trennung von Daten anderer Kunden des IT-Dienstleisters durch virtuelle verschlüsselte Disks getrennt. Personenbezogene Daten werden grundsätzlich nur in den zu den Anwendungssystemen zugehörigen Datenbanksystemen gespeichert. Außer zur Fehleranalyse und ggf. -behebung oder zur Anfertigung von Sicherheitskopien benötigt der IT-Dienstleister keinen Zugriff auf personenbezogene Daten. Die Produktiv- und Testumgebung werden voneinander getrennt.

**2.4. Separation control**

Data from other customers of the IT service provider is separated by virtual encrypted disks. Personal data is only stored in the database systems associated with the application systems. The IT service provider does not require access to personal data except for the purpose of analyzing and, if necessary, rectifying errors or making backup copies. The productive and test environments are separated from each other.

**3. Gewährleistung der Verfügbarkeit und Belastbarkeit**

Die Datenspeichersysteme werden über zwei Standorte gespiegelt und RAID wird eingesetzt. Es erfolgt ein tägliches Backup aller Kundendaten. Die Server werden dabei unterbrechungsfrei mit Strom versorgt. Die Auslegung aller zur Serviceerbringung benötigten Komponenten erfolgt strikt redundant. Wichtige Komponenten werden über zwei gekoppelte -Standorte verteilt. Zur Datensicherung erfolgt ein über mehrere Standorte gespiegeltes Back-Up Verfahren.

**3. Guarantee of availability and resilience**

The data storage systems are mirrored across two locations and RAID is used. All customer data is backed up daily. The servers are supplied with uninterrupted power. The design of all components required for service provision is strictly redundant. Important components are distributed across two linked locations. A mirrored back-up procedure is used for data backup across several locations.

**4. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen**

Die genannten Maßnahmen werden regelmäßig unter Berücksichtigung der einschlägigen technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik überprüft sowie an die sich ändernden bzw. erweiternden IT-Strukturen und geänderten Schutzbedürfnisse und Gefährdungen angepasst.

**4. Procedure for regular review, assessment and evaluation of the effectiveness of the technical and organizational measures**

The aforementioned measures are regularly reviewed, taking into account the relevant technical guidelines and recommendations of the Federal Office for Information Security, and adapted to changing or expanding IT structures and changing protection requirements and threats.

**5. Schriftliche Dokumentation von sonstigen Maßnahmen**

Für die Einhaltung der Richtlinien und Maßnahmen wurde eine Data Security Policy erstellt. Diese Data Security Policy ist verbindlich für alle Mitarbeiter, Gäste und alle Untermieter in den Räumlichkeiten der aufinity Group GmbH. Jeder Verstoß wird beim Vorgesetzten und bei der Geschäftsleitung von aufinity Group GmbH gemeldet und kann geahndet werden.

**5. Written documentation of further measures**

A data security policy has been created to ensure compliance with the guidelines and measures. This Data Security Policy is binding for all employees, guests and all subtenants on the premises of the aufinity Group GmbH. Any violation will be reported to the supervisor and the management of aufinity Group GmbH and may be penalized.

# Anlage 3: Unterauftragsverarbeiter

## Annex 3: Subprocessors

| Unterauftragsverarbeiter<br>*Subprocessor* | Kontakt<br>*Contact* | Beschreibung<br>*Description* | Ort der Verarbeitung<br>*Location of Processing* |
|---|---|---|---|
| Dembach Goo Informatik GmbH & Co. KG | Hohenzollernring 72, 50672 Cologne, Germany<br><br>https://www.dg-i.net/<br>info@dg-i.net | Hosting, Überwachung und Betrieb der Dienste<br>*Hosting, monitoring and operation of services* | Deutschland<br>*Germany* |
| Google Inc. | 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA<br><br>https://www.google.com | Hosting und Cloud Storage<br>*Hosting and Cloud Storage* | USA |
| Mailgun Technologies Inc. | 112 E Pecan St #1135, San Antonio, TX 78205, USA<br>https://www.mailgun.com/ | Parsing und Versand von System-E-Mails<br>*Parsing and sending system e-mails* | USA |
| Functional Software, Inc. | 132 Hawthorne Street, San Francisco, CA 94107, USA<br>www.sentry.io | Erkennung von Code-Fehlern innerhalb der Software für die Systemstabilität unserer Dienste<br>*Detection of code errors within the software for the system stability of our services* | USA |
| Datadog Inc. | 620 8th Avenue, Floor 45, New York, NY 10018, USA | Identifizierung von Code-Fehlern innerhalb der Software für die Systemstabilität unserer Dienste<br>*Identification of code errors within the software for the system stability of our services* | USA |

| | | | |
|---|---|---|---|
| Sensible Technologies Inc. | 1400 Castro St, San Francisco, CA 94114, USA | Strukturierte Auswertung von Rechnungsdaten<br>*Structured processing of invoice data* | USA |
| DigitalOcean LLC. | 101 Avenue of the Americas, 10th Floor, New York, NY 10013, USA https://www.digitalocean.com/ | Benachrichtigung externer Systeme zur Aktualisierung des Status von Transaktionsdaten und Bereitstellung eines verschlüsselten Netzwerks<br>*Notification of external systems to update the status of transaction data and provision of encrypted network* | USA |
| A&O Fischer GmbH & Co. KG | Maybachstraße 9 21423 Winsen (Luhe) | Dienstleister für Briefversand von Post (z.B. Zahlungseinladungen oder Mahnschreiben).<br>*Service provider for sending mail (e.g. payment invitations or reminders).* | Deutschland<br>*Germany* |