Anlage 1 – Technisch organisatorische Maßnahmen nach Art. 28 Abs. 3 lit h, c, 32 DSGVO

Die aufgeführten Angaben beziehen sich auf unseren Hauptstandort in der von-Hünefeld-Str. 3, 50829 Köln. Am Standort befindet sich ebenfalls unser Rechenzentrum.

Die hier beschriebenen Maßnahmen beziehen sich ausschließlich auf diejenigen, die der Auftragnehmer in seinem Unternehmen durchführt. Davon nicht umfasst sind Maßnahmen Dritter, dessen Leistungen der Auftragnehmer auf Weisung des Auftraggebers nutzt. Diese Maßnahmen gelten nicht für Applikationen, die der Auftragnehmer am Markt anbietet und die der Auftraggeber einkauft. Die Unterpunkte b & c sollen nur aufzeichnen welche Daten von Content Partnern verwaltet werden.

1. Technische und organisatorische Sicherheitsmaßnahmen
Gemäß Art. 28 Abs. 3 lit. c, 32 DSGVO sind die Vertragspartner verpflichtet die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

2. Innerbetriebliche Organisation des Auftragnehmers
Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

3. Konkretisierung der Einzelmaßnahmen

Kontrollziele	Maßnahmen
1. Vertraulichkeit, Integrität und Verfügbarkeit	• Überprüfung durch internen Datenschutzbeauftragen
a) Zugangskontrolle <u>Zieldefinition:</u> Verwehrung des Zugangs für Unbefugte zu Datenverarbeitungsanlagen.	• Alarmanlage im Gebäude • Videoüberwachung der Eingänge • Manuelles Schließsystem am Rechenzentrum • Sorgfältige Personalauswahl beim Reinigungsdienst • Regelmäßige Schulungen der Mitarbeiter auf Datenschutz/Informationssicherheit

b)	**Partner für den eMail Content**	• Die Daten werden DSGVO konform in Frankfurt & Amsterdam gespeichert. Ein AV-Vertrag liegt vor.
c)	**Partner für den Ticket Content**	• Die Daten werden DSGVO konform in Frankfurt & Düsseldorf gespeichert. Ein AV-Vertrag liegt vor.
d)	**Transportkontrolle** <u>Zieldefinition:</u> Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.	• Standleitungen werden ausschließlich über IPSec / SSL verschlüsselte Verbindungen realisiert (MPLS / VPN-Tunnel) • Beständige SSL / TLS Transportverschlüsselung. • Einsatz digitaler Zertifikate • Für das Arbeiten außer Haus, Einsatz von VPN
e)	**Eingabekontrolle** <u>Zieldefinition:</u> Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert wurden.	• Protokollierung der Eingabe, Änderung und Löschung von Erfassungsdaten in unserer Software „Kaufmann“ mit eindeutiger Zuordnung des Benutzernamens • Protokolldateien werden anonymisiert abgelegt und bei Bedarf manuell kontrolliert
f)	**Wiederherstellbarkeit** <u>Zieldefinition:</u> Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.	• Das angewandte Datensicherungskonzept beinhaltet inkrementelle, differentielle und Vollsicherungen mit Veeam • Jede erfolgreiche Datensicherung wird stets automatisch überprüft. • Vordefinierte Wiederherstellungsszenarien werden in periodischen Abständen ausgeführt

g) Zuverlässigkeit Zieldefinition: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.	• Überwachung der gesamten IT-Infrastruktur durch ein zentrales und dezentrales Monitoring-System • Existenz eines IT-Notfallhandbuchs mit der Beschreibung einzelner Vorgehensweisen im Ernstfall • Im Fehlerfall werden die Mitarbeiter der IT-Abteilung und weitere dem jeweiligen zugeordneten Dienst per E-Mail informiert
h) Datenintegrität Zieldefinition: Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.	• Betriebssysteme und eingesetzte Softwareprodukte werden stets mit notwendigen Updates versorgt • Es erfolgt der flächendeckende Einsatz eines stetig geupdateten Antivirenprogramms • Einsatz einer Firewall
i) Auftragskontrolle Zieldefinition: Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	• Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten • Schriftliche Weisungen an den Auftragnehmer
j) Verfügbarkeitskontrolle Zieldefinition: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.	• Einsatz einer unterbrechungsfreien Stromversorgung • Einsatz von Überspannungsschutz • Kontinuierliche konsistente Datensicherung • Kontinuierliche Kühlung und Temperaturüberwachung • Einsatz von HC – Clustern • Notfallpläne • Feuerlöscher in unmittelbarer Nähe zum Serverraum

k) Trennbarkeit Zieldefinition: Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.	• Nach Dienst getrennte physische oder virtuelle Systeme • Trennung von Produktiv- und Testsystemen • Strikte Isolation von Datenbänken • Granulare Benutzer- oder Ressourcenberechtigungen für jede Anwendung