Anhang 2 zur Vereinbarung zur Auftragsverarbeitung

Technische und Organisatorische Sicherheitsmaßnahmen gemäß Art. 32 DSGVO

1. Vertraulichkeit

a) Zutrittskontrolle
Um den Zutritt Unbefugter zu den Datenverarbeitungsanlagen mit denen Daten verarbeitet oder genutzt werden zu verhindern, hat DIS duerr-internet-service formale Zutrittskontrollprozesse implementiert.
Der Standort In den Kehlen 4, 97342 Marktsteft beherbergt ein Büro von DIS duerr-internet-service.
Zum Büro hat ausschließlich Wolfgang Dürr Zutritt. Die physikalischen Server stehen als Colocation (selbstverwaltet von DIS duerr-internet-service) bei der STRATO AG, Pascalstraße 10, 10587 Berlin.
Diese Server werden ausschließlich in Deutschland betrieben.
Im Rechenzentrun kommen die standardmäßigen Sicherheitsmaßnahmen zur Anwendung.
Diese erfüllen ein sehr hohes Sicherheitsniveau hinsichtlich physischer Sicherheit, Energieversorgung, Klimatisierung, Netzanbindung, Ausfallsicherheit und Zutrittsregelung, das über die Zertifizierung nach der Sicherheitsnorm ISO/IEC 27001 nachgewiesen werden kann.
Es gibt weder Kollokation noch Serverhousing und entsprechend keinen Zutritt von Dritten (Wartungen etc. ausgenommen, hier gilt allerdings eine Begleitpflicht durch STRATO Mitarbeiter.

b) Zugangskontrolle
Ein Fernzugriff auf Server von DIS duerr-internet-service zu administrativen Zwecken, z.B. zur Wartung der Systeme, ist nur über verschlüsselte Verbindungen und nach vorheriger Authentifizierung möglich.

c) Zugriffskontrolle
Um zu gewährleisten, dass die zur Benutzung eines Systems zur Verarbeitung von Daten Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass gespeicherte oder in Verarbeitung befindliche Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, setzt DIS duerr-internet-service ausschließlich eine Kombination aus Benutzernamen und sicheren Passwörtern (3 aus 4, min. 10 Zeichen) ein. Der Zugriff wird lokal protokolliert. Hierbei werden die gesetzlichen Datenschutzanforderungen, insbesondere solche der Datenschutzgrundverordnung (DSGVO) eingehalten.

2. Trennung
DIS duerr-internet-service verarbeitet die Daten auf Serversystemen, die durch ein System logischer und physischer Zugriffskontrollen im Netzwerk logisch getrennt sind.

3. Integrität

a) Eingabekontrolle
Um zu gewährleisten, dass DIS duerr-internet-service nachträglich überprüfen und feststellen kann, ob und von wem Daten in den Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind, werden alle Zugriffe auf die gespeicherten Daten des Kunden lokal protokolliert.

b) Weitergabekontrolle
Um zu gewährleisten, dass Daten bei der elektronischen Übertragung, während des Transportes oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, an welchen Stellen die Übertragung von

Daten durch Systeme zur Datenübertragung vorgesehen sind, unterliegt der Zugriff auf sämtliche Systeme, die Kundendaten verarbeiten, wirksamen Zugriffskontrollen. Diese Mechanismen zur Zugriffskontrolle sind bereits oben unter 1. näher beschrieben.

3. Verfügbarkeit und Belastbarkeit

DIS duerr-internet-service verwendet in allen Systemen eine Kombination aus redundanten Systemen und Backup Lösungen, um die gespeicherten Daten zu schützen und ggf. wiederherstellen zu können. Diese Systeme werden ausschließlich nach dem aktuellen Stand der Technik gesicherten und ausgestatteten Räumlichkeiten betrieben, die über die notwendige Klimatisierung, Feuer- und Rauchmeldeanlagen verfügen und für die detaillierte Notfallpläne bestehen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Alle Mitarbeiter werden regelmäßig zu Themen des Datenschutzes geschult. Diese Schulungen werden komplett inhouse realisiert, sodass eine genaue Abstimmung auf die bei DIS duerr-internet-service maßgeblichen Fragen möglich ist. Im Rahmen dieser Schulungen werden auch individuelle Fragen eingehend behandelt. Alle Mitarbeiter von DIS duerr-internet-service, die im Rahmen ihrer Tätigkeit mit der Verarbeitung personenbezogener Daten in Berührung kommen sind auf den vertraulichen Umgang mit personenbezogenen Daten verpflichtet. Dies geschieht regelmäßig bereits bei der Einstellung neuer Mitarbeiter mittels einer vertraglichen Verpflichtungserklärung, die jeder Mitarbeiter abzugeben hat.
DIS duerr-internet-service unterhält ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO. Dieses Verarbeitungsverzeichnis ist nicht öffentlich.