Anlage 1:

A. Zu § 2 Art der personenbezogenen Daten

Maßgebliche Datenarten (zB Kontaktdaten) sind:
Name, Adressdaten (postalisch)
E-Mailadresse
Geburtsdatum

Facebook Messenger Daten, das sind:
Facebook-ID
Geschlecht
Sprache
Opt-In für E-Mail Marketing

Buchungs-/Anfragespezifische Daten:
Kategorie der Unterkunft
Anreise-/Abreisedatum
Anzahl der Personen
Anzahl der Kinder
Anzahl der Zimmer
Interesse (Beispiel: Wandern, Mountainbiken, Wellness)

Anmerkung (Wenn der Nutzer eine zusätzliche freitext Anmerkung zur Anfrage hat)

….

B. Zu § 2 Kreis der Betroffenen

Maßgebliche Personengruppen (zB Dienstleister) sind:
Konsumenten

Anlage 2: Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

Dokumentation der nach 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen[1].

1.	**Pseudonymisierung** Wie wird die Pseudonymisierung der Daten gewährleistet? Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.	☒ Data Masking
2.	**Verschlüsselung** Wie wird die Verschlüsselung gewährleistet? Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.	☒ Verschlüsselung von Speichermedien

[1] Dieses Dokument dient der Erfüllung gesetzlicher Anforderungen und soll eine **allgemeine** Beschreibung darstellen, die es ermöglicht, **vorläufig** zu beurteilen, ob die getroffenen Datensicherheitsmaßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages und dem Auftraggeber bei wesentlichen Änderungen und im Übrigen jährlich zur Durchführung der Auftragskontrolle vorzulegen.

3.	**Fähigkeit der Vertraulichkeit** Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet? Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.	☒ Spezielle Schutzvorkehrungen für den Serverraum ☒ Individueller Log-In und Kennwortverfahren ☒ Automatische Sperrung der Clients (Zeitablauf) ☒ Verwaltung von Berechtigungen ☒ Dokumentation von Berechtigungen ☒ VPN (Virtual Private Network) ☒ Gesichertes WLAN ☒ SSL-Verschlüsselung bei Web-Access
4.	**Fähigkeit der Integrität** Wie wird die Fähigkeit der Integrität der Daten dauerhaft gewährleistet? Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.	☒ Verwendung von Zugriffsrechten ☒ Systemseitige Protokollierungen
5.	**Fähigkeit der Verfügbarkeit** Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet? Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.	☒ Back-Up Verfahren ☒ Virenschutz /Firewall
6.	**Fähigkeit der Belastbarkeit** Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet? Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.	☐ Penetrationstests ☐ Sonstige:
7.	**Wiederherstellbarkeit der Verfügbarkeit und des Zugangs** Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?	☒ Notfallplan

8.	**Verfahren zur regelmäßigen Überprüfung** Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?	☒ Sonstige: Stichproben
9.	**Unrechtmäßiger Zugang zu personenbezogenen Daten** Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?	☒ Individueller Log-In und Kennwortverfahren ☒ Automatische Sperrung der Clients (Zeitablauf) ☒ Verwaltung von Berechtigungen
10.	**Verarbeitung personenbezogener Daten nur nach Anweisung** Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen der Verantwortlichen verarbeitet werden?	☒ MitarbeiterInnen sind zu Verhaltensregeln verpflichtet ☒ Implementierung unternehmensinterner Datenschutz-Richtlinien