Technisch-organisatorische Maßnahmen nach Artikel 32 DSGVO

1. Vertraulichkeit

1.1 Zutrittskontrolle

Kein unbefugter Zutritt zu den Datenverarbeitungsanlagen

Alle Gebäude auf dem Firmengelände am Standort der Verwaltung, sowie die einzelnen Bereiche innerhalb der Gebäude, sind durch eine elektronische Zutrittskontrolle geschützt. Hierfür werden Chipkarten in Verbindung mit elektronischen Türöffnern eingesetzt. Durch ein Berechtigungssystem erhalten Mitarbeiter nur Zugang zu den Bereichen, für die sie autorisiert sind. Der Test-Server ist in einem absperrbaren Raum untergebracht. Zudem sind alle Zugänge zu den Gebäuden und relevanten Bereiche der Verwaltung mit einer Zentralschließanlage ausgestattet. Einzelne Bereiche der Gebäude sind jeweils mit einer eigenen Schließung ausgestattet. Es erfolgt eine lückenlose Protokollierung der Schlüsselvergabe und Chipvergabe nach Prüfung der Berechtigung. Das Gelände ist videoüberwacht. Zudem ist ein Schließdienst eingesetzt.

1.2 Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Verschlüsselung von Datenträgern.

- Zugriff auf Desktop-Rechner, Laptop, Notebooks, Mobiltelefone und Server nur mit Passwörtern.
- Sperrung des Benutzerkontos nach drei fehlgeschlagenen Anmeldeversuchen, soweit diese Funktion von der Software unterstützt wird.
- Automatische Sperrung der Desktop Rechner, Laptops, Notebooks, Mobiltelefone bei Inaktivität.
- Verschlüsselung aller mobilen Datenverarbeitungsgeräte und Datenträger.
- Alle Anwendungen sind durch nutzerbezogene Passwörter geschützt.
- Verschlüsselung des Test-Servers
- Die Passwortkomplexität und Länge entspricht den Vorgaben des BSI

1.3 Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

- Anschluss von mobilen Datenträgern und Geräten sowie Nutzung von Disketten oder Optischen Laufwerken durch installierte Software unterbunden.
- Fernwartung zu Wartungszwecken nur innerhalb der Geschäftszeiten und unter Aufsicht.
- Die Anzahl der User mit Administratorrechten ist das Notwendigste reduziert.

1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

- Alle Programme, die zur Verarbeitung von Daten im Auftrag verwendet werden, sind mandantenfähig. Es sind eigene Mandanten für verschiedene Verarbeitungen vorhanden. Es ist über Berechtigungskonzepte gewährleistet, dass Benutzer nur auf die Mandanten zugreifen können, mit deren Bearbeitung Sie vertraut sind.
- Alle Systeme und Anwendungen sind auf eine zweck- und anwendungsbezogene Verarbeitung ausgerichtet. Berechtigungskonzepte und Dienstanweisungen tragen dafür Sorge, dass zu unterschiedlichen Zwecken erhobenen Daten auch getrennt verarbeitet werde.
- Test- und Produktivsysteme sind getrennt.
- Datenbanken der Hotels als getrennte Mandanten

1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Soweit es für eine Verarbeitung der Daten möglich ist erfolgt eine Pseudonymisierung der Daten.
- Es ist gewährleitstet, dass in den jeweiligen Systemen nur die absolut zur Verarbeitung benötigten Daten zur Verfügung stehen.

2. Integrität

2.1 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

- Zugriff auf Programme und Dienste erfolgt ausschließlich über verschlüsselte Verbindungen
- Empfang von Daten von Booking Chanel etc. über Schnittstellen erfolgt über verschlüsselte Verbindungen
- Versand von Daten auf mobilen Datenträgern erfolgt verschlüsselt
- Zugriff auf ibelsa.rooms über verschlüsselte Verbindung
- E-Mail-Transport-Verschlüsselung, soweit von beiden Seiten angeboten

2.2 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

- Die Eingabe, Änderung und Löschung von Daten wird protokoliert.
- Vergabe von Rechten entsprechend dem Berechtigungskonzept
- Die Nachvollziehbarkeit der Eingaben ist durch Vergabe verschiedener Benutzernamen sichergestellt.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.

- Auf allen System sind Virenschutzprogramme und Firewalls aktiv
- Brandmeldeanlage in der Hauptverwaltung mit automatischer Rauchdetektion und Aufschaltung zur Feuerwehr. Brandschutzkonzept.
- Einsatz von Virenschutzsoftware auf allen Clients und Test-Server
- Anschluss von mobilen Datenträgern und Geräten sowie Nutzung von Disketten oder Optischen Laufwerken durch installierte Software unterbunden.
- Dienst- und Arbeitsanweisungen
- Brandmeldeanlage mit automatischer Rauchdetektion und Aufschaltung zur Feuerwehr. Brandschutzkonzept.
- Speicherung der Daten erfolgt in den beauftragten Rechenzentren des Auftragnehmers.
- Dort erfolgt die Sicherung nach Datensicherungskonzept bzw. entsprechend zusätzlicher Anforderungen. Alle Sicherungsvorgänge werden regelmäßig kontrolliert.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management; Incident-Response-Management; datenschutzfreundliche Voreinstellungen; Auftragskontrolle (Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen).

4.1 Datenschutzmanagement

- Es existiert eine für alle Mitarbeiter des Unternehmens verbindliche Datenschutz Compliance. In ihr sind die Zuständigkeiten und Aufgaben der einzelnen Mitarbeiter und Organisationseinheiten in einer Datenschutz Governance Struktur festgeschrieben.
- Regelmäßige Unterweisung der Mitarbeiter in Frontalschulungen
- Regelmäßige Prüfung aller im Verzeichnis der Verarbeitungen aufgeführten Verarbeitungen durch internes Audit durch den Datenschutzbeauftragten.

- Erstellung eines jährlichen Datenschutzberichtes zur Vorlage bei der Geschäftsführung.
- Bestellter Datenschutzbeauftragter
- Regelmäßige Prüfung der getroffenen technischen und organisatorischen Maßnahmen hinsichtlich Ihrer Wirksamkeit und dem Stand der Technik und gegebenenfalls Anpassung der Maßnahmen.
- Verpflichtung auf Verschwiegenheit der Mitarbeiter

4.2 Incident-Response-Management

- Festgelegte Verfahren für die Handhabung von Datenschutzvorfällen und zur Wahrung der Betroffenenrechte. Sowie deren Test.
- Dokumentation der Vorgänge

4.3 Datenschutzfreundliche Voreinstellungen

- Die Grundeinstellungen aller Programme, Dienste und Systeme orientieren sich, so weit technisch möglich, am Grundsatz „Privacy by Default".
- Alle neuen Programme werden vor dem Einsatz auf diese Kriterien hin geprüft und es werden die entsprechenden Einstellungen vorgenommen.

4.4 Auftragskontrolle

- Mit allen Dienstleistern, die Daten im Auftrag verarbeiten und/oder Zugriff auf personenbezogene Daten oder System mit personenbezogenen Daten haben besteht eine Auftragsdatenverarbeitung nach Artikel 28 DS-GVO.
- Verarbeiter im Auftrag werden in regelmäßigen Abständen entsprechend der Vorgaben der DS-GVO geprüft.
- Vor Abschluss von Verträgen mit Dienstleistern erfolgt eine Prüfung der Zuverlässigkeit der Verarbeiter im Auftrag.
- Die Auftragnehmer werden regelmäßig durch Audits überprüft.