Kategorie	Frage	Beschreibung	Ja	Teilweise	Nein	Bemerkungen / Kommentar
Aufbewahrung	Werden personenbezogene Daten und Dokumente ordnungsgemäß (den geltenden Datenschutzgesetzen gemäß) entsorgt und gelöscht?	Betriebsmittel oder Sachmittel (z. B. Druckerpapier, Magnetbänder, Festplatten, CD-ROM , DVD s, USB-Sticks, Flash-Speicher oder -karten) werden irgendwann nicht mehr benötigt oder müssen aufgrund von Defekten ausgesondert werden. Wenn sie personenbezogene Daten enthalten, müssen sie so entsorgt werden, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Ausreichend dimensionierte Dokumentenshredder bzw. externe Entsorger sind zu empfehlen.				
Aufbewahrung	Sind die diversen für Ihre Branche geltenden gesetzlichen Aufbewahrungsfristen bekannt und werden diese eingehalten?	Es existieren verschiedenste Aufbewahrungsfristen, die gesetzlich geregelt sind, z.B. ist eine Rechnung für 7 Jahre aufzubewahren. Andererseits sind personenbezogene Daten, die nicht unter eine gesetzliche Aufbewahrungsfrist fallen, nach Ablauf des legitimen Verwendungszweckes zu vernichten.				
Human Ressources	Gibt es eine kontinuierliche Sensibilisierung bzw. Schulung der Mitarbeiter für den Datenschutz?	Viele Sicherheitsvorfälle werden nicht durch organisationsfremde Angreifer, sondern durch unsachgemäßes Verhalten eigener Mitarbeiter hervorgerufen. Daher sollte Wert darauf gelegt werden, dass alle Mitarbeiter die für ihren Arbeitsplatz erforderlichen Informationssicherheitskenntnisse haben, Zwischenfälle frühzeitig als solche erkennen können und eigenverantwortlich sinnvolle Maßnahmen bei Sicherheitsproblemen ergreifen können.				
Human Ressources	Gibt es (dokumentierte) Regelungen für den Einsatz von Mitarbeitern aus Fremdfirmen, z.B. Wartungstechniker für IT, etc.?	Wie ist mit Mitarbeitern von Fremdfirmen umzugehen? Wie haben sich diese Personen im Unternehmen zu verhalten? Was ist erlaubt, was nicht?				
Human Ressources	Gibt es Vertraulichkeitsvereinbarungen bzw. Geheimhaltungsvereinbarungen?	Diese dienen der Wahrung der Unternehmensgeheimnisse bzw. Unternehmenswerte in Bezug auf interne und externe Personen.				

Kategorie	Frage	Beschreibung	Ja	Teilweise	Nein	Bemerkungen / Kommentar
Human Ressources	Wie werden Bewerbungen bzw. die Einstellung neuer Mitarbeiter durchgeführt?	Was ist beim Eintritt und beim Austritt von Mitarbeitern genau zu beachten und wie ist vorzugehen? Was geschieht mit den Bewerbungsunterlagen? Wie ist HR geregelt bzw. ist HR an Externe outgesourced?				
Human Ressources	Gibt es einen Prozess zur datenschutzgerechten Erfüllung der Betroffenenrechte (Auskunft, Löschung, Widerruf, Widerspruch, Information)?	Gemäß EUDSGVO hat jeder Betroffene das Recht über seine verarbeiteten Daten Auskunft zu verlangen, Löschung zu verlangen, die Verarbeitung zu widerrufen bzw. ihr zu widersprechen und über die Verarbeitung informiert zu werden.				
Human Ressources	Gibt es eine Mitarbeiterrichtlinie zum Datengeheimnis?	Sind die Mitarbeiter Ihres Unternehmens mit PC-Zugang auf das Datengeheimnis verpflichtet?				
IT	Sind die Zugriffs- und Zutrittsrechte für Mitarbeiter und Gäste festgelegt, geregelt, überwacht und dokumentiert (z.B. Mitarbeiter dürfen nur auf jene Daten Zugriff haben, die für die Erfüllung ihres Auftrages notwendig sind)?	Gibt es für jeden Benutzer einen eigenen Account mit den von ihm zur Aufgabenerfüllung benötigten Rechten? Wie werden Rechte festgelegt und vergeben? Werden Benutzeraccounts auch wieder gelöscht, wenn sie nicht mehr benötigt werden (z.B. Austritt des Mitarbeiters)?				
IT	Welche Software/Programme im Unternehmen verarbeiten personenbezogene Daten?	Liste der Applikationen, die personenbezogene und/oder sensible Daten im Sinne des Datenschutzgesetzes verarbeiten.				
IT	Wird im Unternehmen eine Videoüberwachung eingesetzt?	Eine Videoüberwachung im Sinne des österreichischen Datenschutzgesetzes (DSG2000) und der EU Datenschutz Grundverordnung (EUDSGVO) ist ein automationsgestütztes System zur systematischen und fortlaufenden Aufzeichnung oder Weitergabe von Bildern.				
IT	Ist der Einsatz der Videoüberwachung im Unternehmen geregelt und dokumentiert und ist die Einhaltung der Vorgaben gewährleistet?	Der Einsatz einer Videoüberwachung ist exakt zu regeln und zu dokumentieren. Es ist sicherzustellen, dass der Zweck des Einsatzes (theoretisch möglicher Missbrauch genügt) den Vorgaben der Datenschutzbehörde entspricht (z.B. max. Aufbewahrungsdauer von 72 Stunden)				

Kategorie	Frage	Beschreibung	Ja	Teilweise	Nein	Bemerkungen / Kommentar
IT	Welche technischen Einrichtungen und Maßnahmen (zum Datenschutz) sind im Einsatz?	"Privacy by Design". Verwendung von (Key) Kartensystemen, Zutrittssystemen, Zugriffssystemen, WLAN, Netzwerk, Server, Clients, Firewall, Datenverschlüsselung, Protokollierung und Überwachung (Monitoring), Browsereinstellungen, etc. Zugriffe und Rechte regelmäßig kontrollieren.				
IT	Gibt es Regeln & Richtlinien zur Wahrung des Datenschutzes (z.B. Privatnutzung)?	Mitarbeiterrichtlinien für betriebliche Nutzung.				
IT	Gibt es ein Nutzungsverbot nicht-betrieblicher Software und Hardware?	Das Unternehmen ist für alle Programme auf den unternehmenseigenen Rechnern verantwortlich! In unregelmäßigen Abständen sollten die Rechner im Unternehmen auf unzulässige Software überprüft werden; wenn derartige Software gefunden wird, muss sie umgehend deinstalliert werden.				
IT	Gibt es eine Richtlinie für eine Vorgehensweise bei Reparatur oder Ersatz von IT Infrastruktur und wird dabei der Datenschutz berücksichtigt?	Bei Reparatur und Entsorgung (Neuanschaffung) können Daten in unbefugte Hände gelangen.				
IT	Werden Cloud Dienste verwendet?	Bei Cloud Diensten liegen die Daten in den Rechenzentren des Cloud Anbieters. Beispiele dafür sind Office365, Google Drive, OneDrive, Dropbox, etc.				
Marketing	Verfügen Sie über eine zweifelsfreie und schriftliche Zustimmungserklärung aller Personen (intern wie extern), deren personenbezogene Daten Sie verarbeiten, z.B. für Newsletter?	Schriftliche Zustimmungserklärung zur Verarbeitung und Verwendung personenbezogener Daten. Nur gültig, wenn sie freiwillig und in voller Kenntnis der Sachlage bzw. der Risiken gegeben wurde. Falls es einen Betriebsrat gibt, muss die Betriebsvereinbarungspflicht eingehalten werden.				
Marketing	Ist der Widerruf der Zustimmungserklärung möglich, und wenn ja, wie?	Dem Betroffenen ist jederzeit ohne Angabe von Gründen der Widerruf einer Zustimmungserklärung bzw. der Widerspruch zur Verarbeitung seiner personenbezogenen Daten gestattet.				
Marketing	Gibt es Datenschutzerklärungen?	Aufklärung über die Verarbeitung der personenbezogenen Daten inkl. Betroffeneninformation, z.B. Homepage, Newsletter.				

Kategorie	Frage	Beschreibung	Ja	Teilweise	Nein	Bemerkungen / Kommentar
Weitergabe	An wen und wohin werden personenbezogene Daten übermittelt?	An wen erfolgt eine Übermittlung der personenbezogenen und/oder sensiblen Daten im Sinne des Datenschutzgesetzes? Gibt es eine Liste der Empfänger bzw. Empfängerarten?				
Weitergabe	Gibt es Datenübermittlungen bzw. eine Weitergabe von Daten an Drittunternehmen (z.B. externe Personalverrechnung, Skischulen, etc.)?	Datenübermittlung personenbezogener und/oder sensibler Daten an Drittunternehmen.				
Weitergabe	Welche Meldepflichten von personenbezogenen Daten an Behörden und öffentliche Einrichtungen gibt es?	Daten über Gäste oder Mitarbeiter, die an Behörden oder öffentliche Einrichtungen gemeldet bzw. übermittelt werden.				
Dokumentation	Welche Daten mit speziellem Risiko für Betroffene, z.B. Kreditkartendaten, werden verwendet, aufgezeichnet und gespeichert?	Einige Datenarten bergen ein erhöhtes Risiko für Betroffene. Sollten sie bekannt werden, kann für die jeweiligen Betroffenen ein hoher Schaden (finanziell, emotional, Ansehen, etc.) entstehen.				
Dokumentation	Führt Ihr Unternehmen eine Dokumentation der Datensicherheitsmaßnahmen (sog. Datensicherheitskonzept)?	Dokumentationen, Richtlinien, Vorgehensweisen für Datensicherheitsmaßnahmen.				
Dokumentation	Kann Ihr Unternehmen eine Liste der Zugriffsberechtigungen hinsichtlich der relevanten IT Systeme vorlegen?	Dokumentation der Zugriffsberechtigungen und Rollen.				
Dokumentation	Wird die IT Infrastruktur selbst betreut oder von einem Dienstleister?	Auch der Zugriff der Administratoren muss auf ihre Aufgabe beschränkt sein. Weiters sind Administratoren auf ihre speziellen Eigenschaften hinzuweisen und zu schulen.				
Dokumentation	Soweit externe Dienstleister Zugriffsmöglichkeit auf die Daten Ihres Unternehmens haben, wird die Gewährleistung des Datenschutzes durch dieses Drittunternehmen überwacht?	Richtlinie, Verpflichtung und Dokumentation für Drittunternehmen zur Überwachung und Einhaltung des Datenschutzes im Zuge ihrer Tätigkeiten (Auftragsdatenverarbeitervereinbarung, kurz ADV).				
Dokumentation	Welche Arten von personenbezogenen und/oder sensiblen Daten werden gesammelt und verarbeitet?	Art und Umfang von personenbezogenen und/oder sensiblen Daten im Sinne des Datenschutzgesetzes.				

Kategorie	Frage	Beschreibung	Ja	Teilweise	Nein	Bemerkungen / Kommentar
Dokumentation	Gibt es eine Beschreibung (Dokumentation) der Verarbeitung personenbezogener Daten (Verfahrensverzeichnis)?	Wie werden personenbezogene Daten verwendet? Es muss jederzeit auf ein aktuelles Verzeichnis der eingesetzten Hardware, Software und Verfahren sowie der erfassten personenbezogenen Daten zugegriffen werden können.				
Dokumentation	Woher stammen (Quellen) die gesammelten und verarbeiteten Daten?	Woher stammen die im Unternehmen gesammelten und verarbeiteten Daten im Sinne des Datenschutzes (personenbezogene und/oder sensible Daten)? Beispielsweise von den Gästen selbst, von Meldezetteln, aus Reisedokumenten, etc.				
Dokumentation	Gibt es Vorgaben zur Datenträgerverwaltung?	Eine Liste der Datenträger (CD/DVD, USB Stick, Flash Speicher, Datensicherungsbänder, etc.) sollte zu administrativen Zwecken zur Verfügung stehen. Falls es unterschiedliche Aufbewahrungsorte gibt sollte klar ersichtlich sein wo diese aufzufinden sind. Die Backup-Datenträger müssen von den gesicherten Rechnern räumlich getrennt aufbewahrt werden, um zu vermeiden, dass bei einem Brand, Wasserschaden, Einbruch etc. Computer und Datensicherungen gleichzeitig zerstört werden.				
Dokumentation	Ist die Einhaltung der sogenannten "Data Breach Notification Duty" gewährleistet?	Hier handelt es sich um eine Meldepflicht von Datenschutzverstößen. Beispiele dafür sind Datendiebstähle, Verlust von Geräten mit personenbezogenen Daten, unzulässiger Zugriff auf Daten (z.B. durch Wartungstechniker), der Verlust und das mögliche Bekanntwerden vertraulicher Daten oder auch informationstechnische "Einbrüche" (Cyber Attacke). Laut Datenschutzgesetz sind Datenschutzverstöße umgehend an die zuständige Behörde (Datenschutzbehörde) zu melden.				
Dokumentation	Gibt es eine festgelegte und dokumentierte Vorgehensweise beim Eintritt von Notfällen bzw. bei Cyber Attacken?	Unter Notfällen versteht man hier den Verlust von Daten, erfolgreiche Cyber Angriffe von innen oder außen oder auch den Ausfall der IT				