Ergänzung zur Datenverarbeitung

gemäß Art. 28 Abs. 3 der EU-Datenschutz Grundverordnung

1) Zur Erfüllung der vertraglich vereinbarten Geschäftszwecke erfolgt auch die Erhebung, Verarbeitung und Nutzung der übermittelten personenbezogenen Daten nach den einschlägigen gesetzlichen Vorschriften. Personenbezogene Daten sind alle Daten, die auf den Vertragspartner („Kunde“) persönlich beziehbar sind, also z.B. Name, Adresse, E-Mail-Adresse, Zahlungsdaten, bestellte Waren und Dienstleistungen.

2) Verantwortlicher gem. Art. 4 Abs. 7 DS-GVO ist die eventfactory GmbH, Grabenweg 71, 6020 Innsbruck, Österreich.

3) Gem. Art. 6 Abs. 1 f der DS-GVO hat die eventfactory GmbH ein berechtigtes Interesse daran, die an sie übermittelten personenbezogenen Daten, die zum Zweck der Vertragsabwicklung erhoben wurden, auch über die Zeit der Vertragsabwicklung zu speichern, um Ihre Kontaktdaten für zukünftige Aufträge verfügbar zu haben.

4) Der Vertragspartner („Kunde“) hat das Recht, jederzeit gegen die Verarbeitung betreffend personenbezogener Daten, die aufgrund von Art. 6 Abs. f DS-GVO erfolgt, Widerspruch einzulegen und diesen zu begründen.

   Der Widerspruch kann formfrei erfolgen und sollte möglichst via E-Mail an de.datenschutz@liberty-int.com (Datenschutzkoordinator) gerichtet werden.

   Legt der Vertragspartner („Kunde“) Widerspruch ein, werden seine personenbezogenen Daten nicht mehr verarbeitet, es sei denn, die eventfactory GmbH kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten des Vertragspartners („Kunde“) überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

5) Zusätzlich ist die über die Vertragszeit hinausgehende Speicherung für steuerliche Zwecke, zur Geltendmachung von Gewährleistungsansprüchen erforderlich und entspricht damit der Erfüllung einer rechtlichen Verpflichtung unsererseits gem. Art. 6 Abs. 1 c DS-GVO.

6) Der von der Datenverarbeitung Betroffene hat das Recht auf Auskunft nach Art. 15 DS-GVO, das Recht auf Berichtigung nach Art. 16 DS-GVO, das Recht auf Löschung nach Art. 17 DS-GVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO, sowie das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO.

7) Die personenbezogenen Daten des Vertragspartners („Kunde“) werden nicht an Dritte weitergegeben; ausgenommen hiervon ist ausschließlich im Rahmen der Vertragsabwicklung die

Weitergabe an zur Vertragsdurchführung eingeschaltete Dritte (z.B. im Rahmen der Einschaltung Dritter bei Ticketvertrieb nach Ziffer 4.). Eine Übermittlung der Daten an zur Vertragsdurchführung eingeschaltete Dritte erfolgt ebenso nach den gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes 2000 (DSG 2000) und E-Commerce-Gesetz (ECG) sowie der Datenschutzgrundverordnung (DS-GVO). Der Umfang der Übermittlung beschränkt sich auf das notwendige erforderliche Minimum zur Vertragsabwicklung.

8) Der Vertragspartner („Kunde“) hat jederzeit die Möglichkeit, die von ihm gespeicherten Daten ändern oder löschen zu lassen. Das Recht zur Löschung der von ihm gespeicherten Daten besteht nicht, wenn deren Löschung gesetzliche oder vertragliche Aufbewahrungsfristen entgegenstehen, außerdem wenn die Daten für die Begründung, inhaltliche Ausgestaltung oder Änderung sowie Abwicklung des Vertragsverhältnisses zwischen ihm und der Vermittlerin erforderlich sind und für diese Zwecke gespeichert werden müssen.

9) Wenn der Vertragspartner („Kunde“) bei der eventfactory GmbH Dienstleistungen in Anspruch nimmt, werden ihm in Zukunft Informations-E-Mails für ähnliche Dienstleistungen zugesendet. Der Versand dieser E-Mails erfolgt nur nach Abschluss einer Bestellung und unter Einsatz des sog. Double-opt-in-Verfahrens. Das heißt, die Informations-E-Mails werden erst zugesendet, wenn der Vertragspartner („Kunde“) zuvor seine Anmeldung über eine zugesandte Bestätigungs-E-Mail per darin enthaltenem Link bestätigt. Der Vertragspartner („Kunde“) kann jederzeit verlangen, keine solchen Informations-E-Mails mehr zu erhalten. Dazu wendet er sich bitte per E-Mail an De.Datenschutz@liberty-int.com oder an die im Impressum angegebenen Kontaktdaten oder er klickt auf den Link am Ende der Informations-E-Mails.

DATENSCHUTZHINWEISE

Für Kunden und Interessenten

Die eventfactory GmbH ist sich der Bedeutung der personenbezogenen Daten, die ihr anvertraut werden, bewusst. Es ist eine unserer Anliegen, die Vertraulichkeit der Daten sicherzustellen, die uns von Kunden und Interessenten anvertraut werden. Mit den folgenden Informationen möchten wir Ihnen einen Überblick über die Verarbeitung Ihrer personenbezogenen Daten durch uns und Ihre Rechte aus dem Datenschutz nach der EU-Datenschutzgrundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz 2000 (DSG 2000) geben. Welche Daten im Einzelnen verarbeitet und auf welche Weise genutzt werden, richtet sich maßgeblich nach den vereinbarten Leistungen.

A. Verantwortliche Stelle

Verantwortliche Stelle im Sinne der Datenschutz-Grundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz 2000 (DSG 2000) ist:

eventfactory GmbH, Grabenweg 71, 6020 Innsbruck. Österreich

B. Datenschutzkoordinator

Sie erreichen unseren Datenschutzkoordinator unter:

Karin Salota

Email: de.datenschutz@liberty-int.com

C. Quelle der personenbezogenen Daten

Wir verarbeiten personenbezogene Daten, die wir im Zuge unserer Geschäftsbeziehung von unseren Kunden und Interessenten erhalten. Des Weiteren verarbeiten wir – sollte dies für die Erbringung unserer Leistung erforderlich sein – personenbezogene Daten, die wir aus öffentlich zugänglichen Quellen zulässigerweise gewinnen oder die uns von anderen Unternehmen innerhalb der Liberty International Tourism Group Unternehmensgruppe oder von sonstigen Dritten (z. B. einer Auskunft) berechtigt übermittelt werden.

D. Kategorien personenbezogener Daten die verarbeitet werden

Wir verarbeiten folgende Kategorien von personenbezogenen Daten:

- Stammdaten (z.B. Name, Anschrift und Geburtsdatum),
- Kontaktdaten (z.B. Telefonnummer, Emailadresse),
- Daten zur Erfüllung unserer vertraglichen Verpflichtungen (z.B. Umsatzdaten),
- Informationen über Ihre Bonität,
- Korrespondenz (z.B. Schriftverkehr mit Ihnen),
- Werbe- und Vertriebsdaten (z.B. für Sie potenziell interessante Produkte)
- Sowie andere mit den genannten Kategorien vergleichbare Daten.

E. ZWECKE, FÜR DIE DIE PERSONENBEZOGENEN DATEN VERARBEITET WERDEN SOLLEN, UND RECHTSGRUNDLAGEN DER VERARBEITUNG

Wir verarbeiten personenbezogene Daten im Einklang mit den Bestimmungen der EU-Datenschutzgrundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz 2000 (DSG 2000):

1. aufgrund Ihrer Einwilligung (Art. 6 Abs. 1 a DS-GVO)

Soweit Sie uns eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke (z.B. Newsletterversand, Weitergabe von Daten, Auswertung von Zahlungsverkehrsdaten für Marketingzwecke, Lichtbilder im Rahmen von Veranstaltungen) erteilt haben, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung gegeben. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der DS-GVO, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind. Der Widerruf einer Einwilligung wirkt erst für die Zukunft und berührt nicht die Rechtmäßigkeit der bis zum Widerruf verarbeiteten Daten.

2. zur Erfüllung von vertraglichen Pflichten (Art. 6 Abs. 1 b DS-GVO)

Die Verarbeitung von Daten erfolgt zur Erbringung von Dienstleistungen im Rahmen der Durchführung unserer Verträge mit unseren Kunden oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage hin erfolgen. Die Zwecke der Datenverarbeitung richten sich in erster Linie nach dem konkreten Auftragsverhältnis (z.B. Veranstaltungsplanung, Vermittlung). Die weiteren Einzelheiten zu den Datenverarbeitungszwecken können Sie den einzelnen Verträgen und Geschäftsbedingungen entnehmen.

3. aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1 c DS-GVO) oder im öffentlichen Interesse (Art. 6 Abs. 1 e DS-GVO)

Die eventfactory GmbH unterliegt unterschiedlichen rechtlichen Verpflichtungen, das bedeutet gesetzlichen Anforderungen. Zu den Zwecken der Verarbeitung gehören unter anderem die Erfüllung steuerrechtlicher Kontroll- und Meldepflichten und auch die Risikobewertung und -steuerung im Unternehmen und innerhalb der Gruppe.

4. im Rahmen der Interessenabwägung (Art. 6 Abs. 1 f DS-GVO)

Soweit erforderlich verarbeiten wir Ihre Daten über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen von uns oder Dritten. Beispiele:

- Prüfung und Optimierung von Verfahren zur Bedarfsanalyse zwecks direkter Kundenansprache,
- Werbung oder Markt- und Meinungsforschung soweit Sie der Nutzung Ihrer Daten nicht widersprochen haben,
- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten,
- Gewährleistung der IT-Sicherheit und des IT-Betriebs,
- Maßnahmen zur Gebäude- und Anlagensicherheit (z.B. Zutrittskontrollen),
- Maßnahmen zur Sicherstellung des Hausrechts,
- Maßnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten,
- Konsultation von und Datenaustausch mit Auskunfteien zur Ermittlung von Bonitätsrisiken.

F. Weitergabe von Daten

Informationen über unsere Kunden und Interessenten sind wichtig für uns und helfen uns, unser Angebot zu optimieren. Es gehört jedoch nicht zu unserem Geschäft, diese Kundeninformationen zu verkaufen. Innerhalb des Unternehmens sind die Stellen zugriffsberechtigt, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten benötigen.

Die eventfactory GmbH lässt außerdem einzelne der vorgenannten Prozesse und Serviceleistungen durch sorgfältig ausgewählte und datenschutzkonform beauftragte Dienstleister ausführen, die ihren Sitz je nach Ansässigkeit innerhalb der EU oder in einem Drittland haben. Dies sind Unternehmen in den Kategorien IT-Dienstleistungen, Zahlungsverkehr, Abrechnung und Beratung sowie Vertrieb und Marketing sowie Dienstleister, die wir im Rahmen von Auftragsverarbeitungsverhältnissen heranziehen. Im Hinblick auf die Datenweitergabe an weitere Empfänger dürfen wir Informationen über Sie nur weitergeben, wenn gesetzliche Bestimmungen dies erfordern, Sie eingewilligt haben oder wir zur Weitergabe befugt sind. Sind diese Voraussetzungen gegeben, können Empfänger personenbezogener Daten u. a. sein:

- Öffentliche Stellen und Institutionen (z.B. Finanzbehörden) bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung.
- Andere Unternehmen oder vergleichbare Einrichtungen, an die wir zur Durchführung der Geschäftsbeziehung mit Ihnen personenbezogene Daten übermitteln (z. B. Hotels, Transportunternehmen, Restaurant, etc.).
- Andere Unternehmen innerhalb des Konzerns.

Weiterführend können auch andere Stellen Datenempfänger sein, sofern Sie uns Ihre Einwilligung zur Datenübermittlung erteilt haben.

G. Dauer der Datenspeicherung

Wir verarbeiten und speichern Ihre personenbezogenen Daten solange dies für die Erfüllung unserer vertraglichen und gesetzlichen Pflichten erforderlich ist.

Sind die Daten für die Erfüllung vertraglicher oder gesetzlicher Pflichten nicht mehr erforderlich, werden diese regelmäßig gelöscht, es sei denn, deren – befristete – Weiterverarbeitung ist erforderlich zu folgenden Zwecken:

- Erfüllung handels- und steuerrechtlicher Aufbewahrungspflichten. Die dort vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen in der Regel zwei bis zehn Jahre.
- Erhaltung von Beweismitteln im Rahmen der gesetzlichen Verjährungsvorschriften.

H. Rechte als Betroffener

Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 DS-GVO, das Recht auf Berichtigung nach Art. 16 DS-GVO, das Recht auf Löschung nach Art. 17 DS-GVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO, das Recht auf Widerspruch aus Art. 21 DS-GVO sowie das Recht auf Datenübertragbarkeit aus Art. 20 DS-GVO. Darüber hinaus besteht ein Beschwerderecht bei einer zuständigen Datenschutzaufsichtsbehörde (Art. 77 DS-GVO).

Eine erteilte Einwilligung in die Verarbeitung personenbezogener Daten können Sie jederzeit uns gegenüber widerrufen. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der DS-GVO, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

I. Pflichten als Betroffener

Im Rahmen unserer Geschäftsbeziehung müssen Sie diejenigen personenbezogenen Daten bereitstellen, die für die Aufnahme, Durchführung und Beendigung einer Geschäftsbeziehung und zur Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung wir gesetzlich verpflichtet sind. Ohne diese Daten werden wir in der Regel nicht in der Lage sein, einen Vertrag mit Ihnen zu schließen, diesen auszuführen und zu beenden.

J. Bestehen einer automatisierten Entscheidung einschließlich Profiling

Zur Begründung und Durchführung der Geschäftsbeziehung nutzen wir grundsätzlich keine automatische Entscheidungsfindung gemäß Art. 22 DS-GVO. Sollten wir diese Verfahren in Einzelfällen einsetzen, werden wir Sie hierüber gesondert informieren, sofern dies gesetzlich vorgegeben ist. Wir verarbeiten teilweise Ihre Daten automatisiert mit dem Ziel, bestimmte persönliche Aspekte zu bewerten (Profiling). Wir setzen Profiling im Rahmen der Beurteilung Ihrer Zahlungsfähigkeit und zur Verbesserung unserer Vertriebsmaßnahmen ein, um Sie bedarfs und zielgerichteter anzusprechen.

K. Absicht, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln

Eine aktive Übermittlung von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation findet, wenn notwendig, im Rahmen der Vertragserfüllung statt.

WIDERSPRUCHSRECHT

Information über Ihr Widerspruchsrecht nach Art. 21 Datenschutz-Grundverordnung (DS-GVO)

1. EINZELFALLBEZOGENES WIDERSPRUCHSRECHT

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 e DS-GVO (Datenverarbeitung im öffentlichen Interesse) und Art. 6 Abs. 1 f DS-GVO (Datenverarbeitung auf der Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling im Sinne von Art. 4 Nr. 4 DS-GVO. Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

2. WIDERSPRUCHSRECHT GEGEN EINE VERARBEITUNG VON DATEN FÜR ZWECKE DER DIREKTWERBUNG

In Einzelfällen verarbeiten wir Ihre personenbezogenen Daten, um Direktwerbung zu betreiben. Sie haben das Recht, jederzeit Widerspruch gegen die Verarbeitung Sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

Widersprechen Sie der Verarbeitung für Zwecke der Direktwerbung, so werden wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.

Der Widerspruch kann formfrei erfolgen und sollte möglichst gerichtet werden an:

Karin Salota

De.datenschutz@liberty-int.com

Technische und organisatorische Maßnahmen (TOM)

Im Sinne des Art. 32 der Datenschutz-Grundverordnung (DSGVO)

Die Organisation: eventfactory GmbH

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die oben genannte Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

I. Vertraulichkeit

a) Zutrittskontrolle

- Der Zugang zum Büro erfolgt über eine Chip-Karte, einen Zugangscode oder einen manuellen Zugang
- Der Zugang von Gästen zu den Büroräumen erfolgt grundsätzlich innerhalb der Büroöffnungszeiten und unter Aufsicht.
- Es wird eine Liste geführt, welche Personen (Mitarbeiter, Kunden, Partner, Lieferanten) Zugang zu den Büroräumen haben („Schlüsselliste“)
- Sorgfalt bei der Auswahl des Wachpersonals
- Sorgfalt bei der Auswahl des Reinigungspersonals
- Einige Büros sind durch eine Alarmanlage & Videoüberwachung gesichert
- Einige Büros führen ein Besucherbuch

b) Zugangskontrolle

- Der Zugang zu den IT-Systemen erfolgt prinzipiell nur mit einem gültigen Benutzernamen und Passwort
- Die Benutzerpasswörter erfüllen die höchsten Sicherheitskriterien und werden regelmäßig geändert
- Die Passwörter werden nicht auf Papier dokumentiert
- Der Benutzer-Account verfügt über keine lokalen Admin-Rechte. Für Notfälle ist ein lokaler Admin-Account vorhanden, der nur festgelegten Personen bekannt ist.
- Admin-Passwörter werden in einem webbasiertem Passwort-Manager-Online-Dienst dokumentiert
- Der administrative Zugang zu den IT-Systemen erfolgt über personalisierte Benutzer. Sofern es von den Systemen unterstützt wird, erfolgt der Zugang über eine Multi-Faktor-Authentifizierung.
- Existiert eine lokale IT-Infrastruktur, erfolgt der Zugang über einen personalisierten VPN-Zugang
- Der Fade-Out-Prozess von Mitarbeitern ist dokumentiert und der Zugang zum Gebäude bzw. den IT-Systemen wird entsprechend gesperrt

- Zusätzlich zu einem internen Wifi Netzwerk existiert ein separater Gästezugang.
- Sowohl das interne Wifi Netzwerk als auch der Gästezugang sind durch ein gesichertes Passwort geschützt
- Das interne Netzwerk ist durch eine Firewall vom Internet geschützt
- PCs und Laptops sind mit einem stets aktuellen Virenschutz geschützt
- PCs und Laptops werden automatisch mit sicherheitsrelevanten Updates versorgt
- Der Bildschirm auf den PCs und Laptops wird automatisch nach 10 Minuten gesperrt
- Die Vergabe von Berechtigungen erfolgt auf personalisierter Ebene
- Die Notwendigkeit der Berechtigungen wird streng überprüft
- Für die Vergabe von Benutzerberechtigungen ist ein Konzept vorhanden
- Ein Remote-Zugang zu den PCs und Laptops ist für Wartungszwecke/Supportzwecke über TeamViewer erlaubt
- Datenträger werden entsprechend mit BitLocker (Windows) oder FileVault (Apple) verschlüsselt
- Es gibt Richtlinien für die private Nutzung der Firmengeräte
- Es gibt Richtlinien zum Sperren des PCs (manuell wie auch automatisch)
- Mobile Geräte (Smartphones) sind mit einem PIN geschützt
- Mobile Geräte werden gesperrt/gelöscht, sofern der PIN 5-mal falsch eingegeben wird.
- Es gibt Richtlinien für den Umgang mit mobilen Geräten (Smartphones)
- Es gibt Richtlinien für die Ordnung und den Umgang mit Dokumenten am Arbeitsplatzes

c) Zugriffskontrolle

- Analoge Daten werden in absperrbaren Schränken aufbewahrt
- Es existiert ein Berechtigungskonzept
- Die Anzahl der Administratoren wird minimiert
- Die Verwaltung der Benutzerrechte erfolgt ausschließlich durch berechtigte Personen
- Ausbau/Löschung der Festplatten vor der fachgerechten Entsorgung von alten Datenträgern

d) Datenträgerkontrolle

- Die eingesetzten Windows Computern sind mit Bitlocker-Verschlüsselung bzw. mit FileVault, bei Apple-Computern, geschützt.
- Es ist nicht gestattet externen USB Sticks auf den Firmenrechnern zu verwenden

e) Trennungskontrolle

- Bei Beendigung des Auftrages werden alle personenbezogenen Daten, die im Rahmen des Auftrages verwendet wurden, von den Systemen des Auftraggebers gelöscht, sofern es hierfür keinen Grund zur weiteren Aufbewahrung gibt.
- Trennung von Produktiv- und Testumgebung

f) Pseudonymisierung

- Sofern möglich, werden bei der Weitergabe von Daten die Datensätze pseudonymisiert

II. Integrität

a) Weitergabekontrolle

- Personenbezogene Daten werden nur über verschlüsselte Wege übertragen
- Es besteht eine Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
- Wenn möglich, erfolgt eine Weitergabe in anonymisierter oder pseudonymisierter Form
- Eine persönliche Übergabe erfolgt nur mit einem Protokoll
- Im Support-Fall werden nur die personenbezogenen Daten weitergegeben, die zur Lösung von Problemen notwendig sind. Die Weitergabe erfolgt per Email oder in den dafür vorgesehenen Support-Plattformen der jeweils betroffenen Systeme
- Es werden keine Passwörter von Kunden auf elektronischem Wege übermittelt

b) Eingabekontrolle

- Es erfolgt eine technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Die Eingabe, Änderung oder Löschung von personenbezogenen Daten in den Systemen erfolgt ausschließlich durch berechtigte Personen
- Die Eingabe, Änderung oder Löschung von personenbezogenen Daten in den Systemen wird dokumentiert
- Der Zugang zu den Dokumentationen ist nur berechtigten Personen vorbehalten
- Es gibt eine klare Regelung der Zuständigkeiten für die Löschung der Daten

c) Benutzerkontrolle

- Die PCs und Laptops sind mit einem automatischen Sperrbildschirm versehen, der sich nach 10 Minuten aktiviert
- Die Mitarbeiter sperren die eingesetzten Computer und Laptops beim Verlassen des Arbeitsplatzes
- Eingesetzte Smartphones sind mit einem PIN geschützt

III. Verfügbarkeit und Belastbarkeit – Kriterien bei einer Cloud Infrastruktur

- Die verwendeten Computer sind mit einem aktuellen Virenschutz ausgestattet. Dieser wird regelmäßig und automatisch aktualisiert (Sicherheitsupdates)
- Verlässt ein Mitarbeiter das Unternehmen bzw. wird ein Vertrag mit einem Subunternehmer beendet, so werden die Zugänge zu den Systemen umgehend gelöscht
- Es werden nur Cloud-Dienste renommierter Hersteller wie z.B. Microsoft eingesetzt
- Es ist ein Backup & Wiederherstellungskonzept vorhanden
- Der Erfolg der Sicherung wird kontrolliert
- Ein Notfallplan ist vorhanden
- Daten werden wie folgt gesichert
    - Filedaten
    - Maildaten
    - Applikationsdaten
- Es sind Wartungsverträge mit den Systemlieferanten vorhanden bzw. mit externen IT-Unternehmen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Datenschutz-Management

- Die Mitarbeiter werden regelmäßig auf den DSGVO-konformen Umgang mit personenbezogenen Daten und IT - Sicherheit geschult
- Es stehen den Mitarbeitern bzw. Subunternehmen entsprechende Richtlinien für den Umgang mit personenbezogenen Daten zur Verfügung.
- Die Mitarbeiter sind zur Geheimhaltung bzw. Verschwiegenheit verpflichtet und haben dies in einer Mitarbeiter-Datenschutzerklärung schriftlich bestätigt.
- Eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz stehen den Mitarbeiter zur Verfügung.
- Die Überprüfung der Wirksamkeit der technischen Schutzmaßnamen wird 1 x pro Jahr durchgeführt
- Es gibt einen internen Datenschutzkoordinator
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 der DSGVO nach
- Ein vorgegebener Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

b) Unterstützung bei der Reaktion auf Sicherheitsverletzungen

- Es besteht ein dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen, auch in Hinblick auf die Meldepflicht gegenüber der Aufsichtsbehörde
- Es bestehen dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Es besteht eine Dokumentation von Sicherheitsvorfällen und Datenpannen
- Ein bestehen ein formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

c) Datenschutzfreundliche Voreinstellungen

- Es werden, sofern von den Systemen unterstützt, datenschutzfreundliche Voreinstellungen vorgenommen, wie z.B. die Multi-Faktor-Authentifizierung bei administrativen Benutzern. Ebenso werden komplexen Passwörter, sowie die Verwendung der Bitlockerverschlüsselung eingesetzt.
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

d) Auftragskontrolle

- Datenverarbeitung findet im Sinne von Art. 28 DSGVO statt, sofern es eine dokumentierte Weisung des Verantwortlichen gibt. Diese ist entweder im Auftrag festgehalten, oder wird schriftlich im Einzelfall bzw. bei Projekten übermittelt. Im Rahmen von regelmäßig standfindenden Besprechungen werden der Status bzw. die notwendigen Maßnahmen besprochen und Verbesserungen vorgeschlagen.
- Es wird vom Kontrollrecht gegenüber der Dienstleister entsprechender gebraucht gemacht
- Die getroffenen Sicherheitsmaßnahmen (TOMs) und deren Dokumentation wird geprüft
- Dienstleister werden unter Sorgfaltsgesichtspunkten ausgewählt
- Sofern notwendig sind entsprechende Vereinbarungen abgeschlossen worden (Geheimhaltungspflicht, Auftragsverarbeiter-Vertrag, EU-Standard-Vertragsklauseln).