Technische und Organisatorische Maßnahmen (Security Policy)

Präambel

Axess gewährleistet die folgenden IT-Sicherheitsmaßnahmen im Rahmen der Kundenbeziehung.

1. Allgemeine technische und organisatorische Maßnahmen

Axess ergreift stets alle für die Verarbeitung der übermittelten Daten in den Datenverarbeitungssystemen erforderlichen Maßnahmen in Übereinstimmung mit der DSGVO und gewährleistet, dass die interne Organisation so gestaltet ist, dass sie den Anforderungen des Datenschutzes entspricht. Die folgenden Bestimmungen gelten unabhängig davon, wo der Server gehostet wird.

1.1. Kontrolle des Verwendungszwecks

Durch die folgenden Maßnahmen wird sichergestellt, dass die für unterschiedliche Zwecke erhobenen Daten getrennt verarbeitet werden:

- softwarebasiert (z.B. Kundentrennung)
- Trennung durch Zugriffsregelung (Datenbankprinzip)
- Trennung von Test- und aktuellen Daten
- Trennung von Test- und laufenden Systemen (Technik, Programme)

1.2. Pseudonymisierung

Soweit für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und separat gespeichert.

1.3. Eingabekontrolle

Es ist gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus diesen entfernt werden. Axess wird zu diesem Zweck Eingaben/Logfiles dokumentieren bzw. aufzeichnen.

1.4. Privacy by Design & Privacy by Default

Durch entsprechende Voreinstellungen im Rahmen der technischen und organisatorischen Maßnahmen ist sichergestellt, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweils angegebenen Verarbeitungszweck erforderlich ist.

- Personenbezogene Daten werden nur dann erhoben, wenn sie für die Abwicklung des Kaufvertrages (z.B. Dauerkarten) notwendig sind.
- Das Setzen von Cookies in Axess Webshops ist nur mit Zustimmung des Nutzers möglich.
- Die Nutzung der personenbezogenen Daten zu Marketingzwecken ist nur mit aktiver Zustimmung des Nutzers zulässig.

2. Technische und organisatorische Maßnahmen bei Server-Hosting durch Axess

Wird im Rahmen des Kaufvertrages die Leistung des Data Center Service bezogen, so ist sichergestellt, dass Sicherheitsbereiche und der Kreis befugter Personen bzw. Zutrittsberechtigungen festgelegt, Zugangswege entsprechend abgesichert, sowie Datenträger kontrolliert und gesichert aufbewahrt werden. Die folgenden Maßnahmen gelten nur, wenn der Server von Axess gehostet wird.

2.1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, in denen Daten verarbeitet werden untersagt. Die Rechnerräume befinden sich in einem Bürogebäude, das als erdbebensicher eingestuft ist. Nur Mitarbeiter der IT, Facility und der Geschäftsleitung haben Zugang zu den Räumlichkeiten. Die Zutrittskontrolle wird durch die folgende Maßnahme gewährleistet:

- Berechtigungs-/Chipkarte

Die Anwesenheit in der Sicherheitszone wird registriert. Nicht autorisiertes Personal und betriebsfremde Personen (Servicetechniker, Berater, Reinigungspersonal, etc.) dürfen die Räume nur in Begleitung von autorisierten Personen betreten. Die Zutrittskontrolle wird durch folgende weitere organisatorische/technische Maßnahmen unterstützt:

- Alarmanlage
- Gebäudeüberwachung
- Videotechnik

2.2. Zugangskontrolle

Eine Nutzung der Datenverarbeitungssysteme durch Unbefugte wird durchfolgende Maßnahmen verhindert:

- Passwort
  Jede berechtigte Person hat ein eigenes, nur ihr bekanntes Passwort, das in regelmäßigen Abständen geändert werden muss. Über alle Aktivitäten an der Datenverarbeitungs- und Telekommunikationsanlage werden automatische Protokolle (Logfiles) erstellt.

Die Nutzung von Datenverarbeitungssystemen mit Hilfe von Geräten zur Datenübertragung durch Unbefugte wird durch folgende Maßnahmen verhindert:

- VPN (Virtuelles Privates Netzwerk)

2.3. Zugriffskontrolle

Es wird sichergestellt, dass die zur Nutzung einer Datenverarbeitungsanlage berechtigten Personen ausschließlich auf ihre zugriffsberechtigten Daten zugreifen können und dass Daten während der Verarbeitung, Nutzung sowie Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Beschränkung der Zugriffsmöglichkeit des Berechtigten auf die ausschließlich seiner Zugriffsberechtigung unterliegenden Daten wird durch folgende Maßnahmen gewährleistet:

- Automatische Überprüfung der Zugriffsberechtigung (im System)

2.4. Übermittlungskontrolle

Es ist gewährleistet, dass personenbezogene Daten bei der elektronischen Übermittlung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, zu welchem Zeitpunkt eine Übermittlung personenbezogener Daten durch Geräte zur Datenübermittlung vorgesehen ist. Der Versand von Datenträgern wird durch Anmelde- und Begleitpapiere dokumentiert und kontrolliert. Es ist nicht gestattet, private Datenträger in die Räume mitzubringen und zu nutzen. Datenträger werden auf folgende Weise vernichtet:

- Magnetische Datenträger durch Überschreiben und physische Vernichtung (externer Dienstleister)

Soweit das Internet zur Übermittlung personenbezogener Daten genutzt wird, werden folgende Sicherheitsmaßnahmen eingesetzt:

- Firewall
- VPN (Virtuelles Privates Netzwerk)

2.5. Verfügbarkeitskontrolle

Durch folgende Maßnahmen wird sichergestellt, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind:

- tägliche/wöchentliche/monatliche/jährliche Datensicherung
- SAN (Speicherbereichsnetzwerk)
- Plattenspiegelung (RAID u.a.)
- USV (unterbrechungsfreie Stromversorgung)
- Überspannungsfilter
- Notstromaggregat
- Auslagerung von Daten
- Feuerschutzeinrichtungen

2.6. Datenschutzmanagement

Es ist sichergestellt, dass ein Datenschutzmanagement eingerichtet und umgesetzt wird. Das Datenschutzmanagement gliedert sich in die folgenden Punkte:

- Verzeichnis der Verarbeitungstätigkeiten
- Auftragsdatenverarbeitung
- Datenschutz-Folgenabschätzung
- Management der Reaktion auf Vorfälle
- Meldung von Datenschutzverstößen
- Fortbildungen
- PDCA (Plan, Do, Check, Act): regelmäßige Kontrollen

2.7. Vorfall-Management

Es wurden Maßnahmen getroffen, wie die Verantwortlichen auf mögliche Szenarien reagieren sollen. Dazu gehören Datensicherheitsverletzungen, DoS (Denial of Service), DDoS (Distributed Denial of Service), Lücken in der Firewall, Ausbrüche von Viren oder Malware und Bedrohungen durch Insider. Das Incident Response Management gliedert sich in sechs wichtige Phasen:

- Vorbereitung: Sowohl die Benutzer als auch die IT-Mitarbeiter werden geschult oder darüber informiert, dass potenzielle Vorfälle auftreten und welche Schritte eingeleitet werden müssen.
- Identifizierung: Feststellung, ob es sich bei einem Ereignis um einen Datenschutzvorfall handelt.
- Eingrenzung: Begrenzung der durch den Vorfall verursachten Schäden und Isolierung der betroffenen Systeme, um weitere Schäden zu vermeiden.
- Beseitigung: Ermitteln der Ursache oder des Auslösers des Vorfalls und Entfernen der betroffenen Systeme aus der Produktivumgebung.
- Wiederherstellung: Betroffene Systeme wieder in die produktive Umgebung integrieren, nachdem sichergestellt wurde, dass keine weiteren Bedrohungen bestehen.
- Erkenntnisse: Vervollständigung der Vorfallsdokumentation und Analyse, was das Team oder das Unternehmen aus dem Vorfall lernen kann. Auf diese Weise können künftige Reaktionen unter Umständen verbessert werden.

3. Zugriff auf Kundendaten

Um bei Problemen angemessenen Support leisten zu können, behält sich Axess als Datenverarbeiter das Recht vor, auf das System oder die Daten des Kunden zuzugreifen, sofern ein solcher Zugriff durch den Kaufvertrag zwischen Axess und dem Kunden abgedeckt ist oder der Kunde einem solchen Zugriff zugestimmt hat, oder der Reseller den gewünschten Serviceantrag im Namen des Kunden an Axess weitergeleitet hat. Axess garantiert, dass:

- ein physischer Zugriff auf die Hardware des Rechenzentrums nur erfolgt, wenn der Kunde den Data Center Service von Axess bezieht;
- der Zugriff auf die Daten des Kunden über das Fernwartungstool nur in dem oben beschriebenen Fall und mit Zustimmung oder im Auftrag des Resellers und/oder des Kunden erfolgt;
- der Zugriff auf lokale Geräte nur im Supportfall auf Anfrage des Kunden oder des Resellers gewährt wird.

4. Auftragsverarbeitungskontrolle

Axess unterhält Verträge mit externen Parteien für die folgenden Arten der Auftragsdatenverarbeitung:

- Datenverarbeitung durch Externe
- Datenträgervernichtung / Entsorgung durch Externe
- Wartung und Fernwartung durch Externe
- Administration / Fernadministration durch Externe

Die Verarbeitung personenbezogener Daten wird durch folgende Maßnahmen gewährleistet:

- schriftliche Weisungen
- Angebots- und Auftragsbestätigung
- Pseudonymisierung

Axess bindet Unterauftragsverarbeiter nur nach vorheriger Prüfung und Freigabe ein und berücksichtigt dabei deren Eignung im Hinblick auf Datenschutz und Informationssicherheit. Die Einbindung erfolgt auf Grundlage geeigneter vertraglicher Regelungen, insbesondere durch Abschluss von Auftragsverarbeitungsverträgen oder vergleichbarer Vereinbarungen. Axess überprüft vor der Beauftragung sowie in angemessenen Abständen während der Vertragslaufzeit, ob geeignete technische und organisatorische Maßnahmen umgesetzt sind, und überwacht die Einhaltung der vereinbarten Datenschutz- und Sicherheitsstandards.