shore.com

Technische und organisatorische Maßnahmen

Kategorien

01. Allgemeine Informationen 2

02. Zutrittskontrolle 4

03. Zugangskontrolle 5

04. Zugriffskontrolle 5

05. Weitergabekontrolle 7

06. Eingabekontrolle 7

07. Auftragskontrolle 8

08. Verfügbarkeitskontrolle 9

09. Trennungsgebot 10

01. Allgemeine Informationen

Anforderung und Handhabung

Hosting und Infrastruktur Übersicht

Die IT-Infrastruktur der Shore GmbH besteht 1. Aus angemieteten Servern im Rechenzentrum eines Internet Service Providers (im Folgenden ISP) sowie 2. aus eigenen Servern und Computern in den Büroräumen (Desktops, Laptops). Dabei dienen die beim ISP angemieteten Server gleichermaßen dem Zweck der Entwicklung (z.B. Datenaufbereitung, Datenintegration, Programmierung, Softwaretesting) wie auch der Bereitstellung der gemäß Auftrag bzw. Lizenzvereinbarung erworbenen SaaS-Anwendung (im Folgenden Software) an den Auftraggeber. Die eigenen Server und Computer der Shore GmbH dienen ausschließlich dem Zweck der internen Ablage (z.B. Personalakten, Datenaufarbeitung im Auftrag des Kunden). Es erfolgt keine Speicherung auf Computern (Desktops, Laptops). Dazu wird jedem Mitarbeiter, der mit der Verarbeitung der Daten beauftragt ist, von einem Systemadministrator der Shore GmbH ein eigener verschlüsselter Speicher zugewiesen, worauf nur der Systemadministrator und dieser Mitarbeiter Zugriff hat. Auf diesem Speicher werden nur solche Dateien abgelegt, die der Mitarbeiter für seine Arbeit im Rahmen der Auftragsbearbeitung benötigt. Ferner wird einzelnen Teams bzw. Mitarbeitergruppen ein gemeinsamer Speicher zugewiesen, sodass gemäß den Berechtigungen eine Verarbeitung erfolgt. Der Zugriff auf die zu verarbeitenden Daten ist ausschließlich aus dem internen Netzwerk in den Büroräumen vor Ort möglich und zusätzlich durch Passwörter geschützt.

Der Zugriff auf das interne Netzwerk aus anderen Netzwerken kann nur über eine autorisierte und verschlüsselte VPN Verbindung erfolgen. Alle Server und Computer werden durch die Shore GmbH selbst administriert. Alle angemieteten Server der Shore GmbH sind in Rechenzentren in der Bundesrepublik Deutschland, alle eigenen Server in den gesicherten Büroräumen der Shore GmbH in München verortet. Zugriffe auf personenbezogene Daten finden nur statt, sofern diese für die Bereitstellung der Software zwingend erforderlich sind. Zur Entwicklung wird mit simulierten Testdaten gearbeitet, die keinen Personenbezug aufweisen. Der Zugriff auf die verarbeitenden Softwareprogramme ist sowohl aus dem internen Netzwerk als auch über das Internet möglich. Der Zugriff auf die verschlüsselten Speicher ist durch Passwörter, individuelle Zugriffsschlüssel, Firewalls, SSL, VPNs und vergleichbare Sicherheitsmaßnahmen geschützt.

Server und Webhosting

Die angemieteten Server sind bezüglich Integrität und Verfügbarkeit ausreichend durch das jeweilige Rechenzentrum, welches eine Zertifizierung mindestens nach ISO 27001 vorweist, geschützt. Ein entsprechender Nachweis der Zertifizierung liegt vor und wird dem Auftraggeber auf Verlangen zur Verfügung gestellt. Die angemieteten Server werden vollständig durch die Shore GmbH administriert.

Zugriff auf personenbezogene Daten nur auf Anweisung

Zugriff auf personenbezogene Daten erfolgt nur auf Anweisung. Sofern diese zur Bereitstellung sowie Wartung der Software zwingend erforderlich sind. Der Zugriff wird nur aufgrund der Festlegung der Zugriffsberechtigung und des Berechtigungskonzepts gewährt. Zur Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS

GVO stellt der Auftragnehmer sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter auf die Vertraulichkeit verpflichtet wurden sowie zuvor und regelmäßig zu Datenschutz und Datensicherheit geschult werden.

✓ **Mobile Device Management**

Endgeräte vom Typ Apple MacOS und Microsoft Windows werden zentral durch die IT der Shore GmbH verwaltet. Alle eingesetzten Systeme verfügen über Virenscanner und softwaregestützte Firewalls. Die Vergabe, der Entzug und die Veränderung von Zugriffsberechtigungen im MDM werden dokumentiert und alarmieren die IT. Alle Computer von Mitarbeitern, die Zugriff auf Daten und Softwareprogramme haben, sind dem Stand der Technik entsprechend verschlüsselt sowie mit Viren-Scanner und Personal Firewalls ausgestattet.

✓ **Remote Verwaltung und Löschung Endgeräte im Verlustfall**

Alle Geräte des Typs Apple MacOS und Microsoft Windows können remote zurückgesetzt und formatiert werden.

✓ **Virenscanner und Firewalls Mobile Device Management**

Eingesetzte Endgeräte von MacOS und Windows verfügen über Virenscanner und softwaregestützte Firewalls.

✓ **Datenverschlüsselung**

Shore verschlüsselt Daten In-Transit, At-Rest, In-Application. Alle Datenübertragungen sind durch TLS 1.2 mit AES-256 geschützt. Alle gespeicherten Daten werden nach dem Industriestandard AES verschlüsselt, der Schlüssel ist ausschließlich Shore bekannt.

✓ **Webhosting verschlüsselte Datenübertragung**

Im Rahmen unseres Produktes findet eine Datenübertragung an die Nutzer der Applikation statt. Diese erfolgt im Browser verschlüsselt gemäß dem aktuellen Stand der Technik. Für alle Datentransporte werden SSL/TLS Zertifikate genutzt. Datentransfer wird durch TLS 1.2 mit AES-256 geschützt.

✓ **Webhosting verschlüsselte Datenspeicherung**

Alle gespeicherten Daten werden nach dem Industriestandard AES verschlüsselt.

02. Zutrittskontrolle

Anforderung und Handhabung

✓ **Automatisches Zugangskontrollsystem**

Jeder Mitarbeiter bekommt einen RFID Token um Zugang zum Büro zu erlangen. Zugang ohne Token ist nicht möglich. Jeder Zugang wird protokolliert. Zugänge werden zeitlich begrenzt, so dass ein Zugang außerhalb der Öffnungszeiten und am Wochenende nur autorisierten Mitarbeitern gewährt wird. Zutritt zum Büro ist ausschließlich für Mitarbeiter und Vor-Ort-Personal sowie in Begleitung eines Mitarbeiters möglich.

✓ **Schlüsselregelung (Schlüsselausgabe etc.)**

Schlüssel werden als RFID Token vergeben. Zugang ohne Token (Schlüssel) ist nicht möglich. Zugänge sind für jeden Mitarbeiter zeitlich begrenzt.

✓ **Protokollierung der Besucher**

Alle Zugänge von den Mitarbeitern der Shore GmbH zu Büro Räumen werden durch Schlüssel Tokens mit RFID Chip gewährt und protokolliert. Zutritt zum Büro ist ausschließlich für Mitarbeiter und Vor-Ort-Personal sowie in eingeladenen Besuch in Begleitung eines Mitarbeiters möglich. Der Besuch wird durch den einladenden Mitarbeiter an der Tür abgeholt und hält sich
ausschließlich in für den Besuch benötigten Räumen in Begleitung eines Mitarbeiters auf.

✓ **Manuelles Schließsystem**

Alle Eingangstüren sind ausschließlich mit RFID Schlüssel zu öffnen. Des Weiteren besteht ein Zugang über die Lasten Aufzüge durch den Einsatz herkömmlicher Schlüssel. Die Ausgabe von den herkömmlichen Schlüsseln erfolgt ausschließlich bei gegründetem Bedarf, nur an Personen, welche eine leitende Position bekleiden. Die Ausgabe wird dokumentiert und überwacht.

✓ **Personen-kontrolle beim Pförtner/Empfang**

Zutritt zum Büro ist ausschließlich für Mitarbeiter und Vor-Ort-Personal sowie eingeladene Besucher möglich. Der Besuch wird durch den einladenden Mitarbeiter an der Tür abgeholt und hält sich ausschließlich in für den Besuch benötigten Räumen in Begleitung eines Mitarbeiters auf.

✓ **Sorgfältige Auswahl von Reinigungspersonal**

Das Reinigungspersonal wird sorgfältig ausgewählt und überprüft. Zudem besteht eine Geheimhaltungsvereinbarung sowie detaillierte Anweisungen in Bezug auf Zugang und Verhalten während der Tätigkeitsausübung.

03. Zugangskontrolle

Anforderung und Handhabung

✓ **Authentifikation mit Benutzername/Passwort**

Mitarbeiter verfügen über eigene passwortgeschützte Zugänge zu Systemen. Diese Zugänge sind beschränkt auf die jeweiligen Aktivitäten nach dem "Need to Know" Prinzip. Wenn möglich wird Single Sign On genutzt um Zugänge zentralisiert zu verwalten und schnelle Deprovisionierung zu ermöglichen. Sämtliche Anwendungen werden mit Nutzername und Passwort Authentifizierung genutzt.

✓ **Einsatz von Intrusion-Detection-Systemen**

✓ **Einsatz von Anti-Viren-Software**

Auf allen Servern und Computern ist eine Antivirus-Software installiert.

✓ **Einsatz einer Hardware-Firewall**

Es wird eine Firewall eingesetzt.

✓ **Einsatz von VPN-Technologie**

Die VPN-Lösung verwendet L2TP mit IPsec-Verschlüsselung.

✓ **Einsatz einer Software-Firewall**

04. Zugriffskontrolle

Anforderung und Handhabung

✓ **Arbeitsplatz Clean Desk Policy**

Am Ende des Arbeitstages werden die Computerarbeitsplätze gesichert. Sobald ein Arbeitsplatz für längere Zeit nicht besetzt ist: Alle sensiblen und vertraulichen Dokumente müssen vom Schreibtisch entfernt und in eine Schublade oder einen Rollcontainer verstaut werden. Sobald der Arbeitsplatz verlassen wird, müssen PC und andere Geräte gesperrt werden. PC und Geräte können nur durch Passwort oder Biometrie entsperrt werden.

✓ **Erstellen von Benutzerprofilen**

Nur geschulte Mitarbeiter bekommen Benutzerprofile in Hosting und Infrastruktur nach dem "Need to Know Principle". Periodisch werden Benutzerrechte und Benutzerprofile überprüft und Zugänge verwehrt oder gewährt.

✓ **Zuordnung von Benutzerprofilen zu IT-Systemen**

Benutzer besitzen nur Zugriffsberechtigungen auf Daten, die zur Ausübung ihrer Tätigkeit notwendig sind (Differenzierte Berechtigungen und Berechtigungskonzepte z.B. Benutzerprofile, Rollen, Begrenzter Zugriff auf Ordner)

✓ **Zuordnung von Benutzerrechten**

Nur geschulte Mitarbeiter bekommen Benutzerprofile in Hosting und Infrastruktur nach dem "Need to Know Principle"". Periodisch werden Benutzerrechte und Benutzerprofile überprüft und Zugänge verwehrt oder gewährt."

✓ **Verwaltung der Rechte durch Systemadministrator**

Rechte innerhalb des Berechtigungskonzeptes werden von Systemadministratoren und Management vergeben.

✓ **Passwortvergabe**

Mitarbeiter verfügen über eigene passwortgeschützte Zugänge zu Systemen. Diese Zugänge sind beschränkt auf die jeweiligen Aktivitäten nach dem "Need to Know" Prinzip. Wenn möglich wird Single-Sign-On genutzt um Zugänge zentralisiert zu verwalten und schnelle Deprovisionierung zu ermöglichen. Sämtliche Anwendungen werden mit Nutzername und Passwort Authentifizierung genutzt. Diese Passwörter bestehen stets aus Zahlen und Buchstaben, das Passwort muss alle 90 Tage geändert werden. Anmeldeversuche und erfolgreiche Anmeldungen in die Software werden protokolliert

✓ **Begrenzung der Anzahl vergebener Administratorenrechte**

Admin Berechtigungen werden nach dem "Need to Know Principle" vergeben und regelmäßig als Teil des Berechtigungskonzeptes und dessen Rollen überprüft

✓ **Protokollierung von Zugriffen auf Anwendungen**

Protokollierung von Zugriffen auf Anwendungen.

✓ **Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)**

Es werden DSGVO-Konforme Aktenvernichter eingesetzt. Die verschlossene Vernichtungstonne wird durch einen ausgewählten Dienstleister entsorgt.

✓ **Ordnungsgemäße Vernichtung von Datenträgern**

Datenträgerentsorgung erfolgt durch 3-fache Überschreibung (5220.22-M-Standard des US-Verteidigungsministeriums).

05. Weitergabekontrolle

Anforderung und Handhabung

- ✓ **Einrichtungen von Standleitungen bzw. VPN-Tunneln**
- ✓ **E-Mail-Verschlüsselung**
- ✓ **Auftragsverarbeiter werden geprüft und sind durch entsprechende AVV an die Vorgaben von Shore gebunden**

  Ja, bestehende AVVs werden durch den Datenschutzbeauftragten zeitnah überprüft
- ✓ **Beim physischen Transport: Sorgfältige Auswahl von Transportpersonal**
- ✓ **Nutzung von Daten in anonymisierter Form**
- ✓ **Beim physischen Transport: sichere Transportbehälter/-verpackungen**

06. Eingabekontrolle

Anforderung und Handhabung

- ✓ **Protokollierung der Eingabe, Änderung und Löschung von Daten**

  Protokollierung von Eingabe, Änderung und Löschung von Daten erfolgt.
- ✓ **Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)**

  Eingabe, Änderung und Löschung durch Shore ist nur mit der richtigen Rollenzuweisung möglich. Berichtigte Mitarbeiter verfügen über personalisierte Zugänge.
- ✓ **Vergabe von Rechten zur Eingabe, Änderung und Löschung**

  Erfolgt auf Basis des Berechtigungskonzepts

- ✓ **Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen**
- ✓ **Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.**

07. Auftragskontrolle

Anforderung und Handhabung

- ✓ **Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)**

  Ja, Vertragsprüfung
- ✓ **Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)**
- ✓ **Auftragnehmer hat Datenschutzbeauftragten bestellt**
- ✓ **Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart**
- ✓ **Vertragsstrafen bei Verstößen**
- ✓ **Prüfung der vom Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen**
- ✓ **Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis**
- ✓ **Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags**
- ✓ **Regelmäßige Überprüfung des Auftragnehmers und seiner Tätigkeiten**

08. Verfügbarkeitskontrolle

Anforderung und Handhabung

✓ **Unterbrechungsfreie Stromversorgung (USV) im Serverzentrum**

Webhosting ist durch redundante Netzersatzanlage gesichert.

✓ **Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen**

✓ **Feuer- und Rauchmeldeanlagen für Serverräume**

✓ **Alarmmeldung bei unberechtigten Zutritten zu Serverräumen ISP**

Der physische Zugang wird durch professionelles Sicherheitspersonal an den Gebäudeeingängen kontrolliert. Dabei werden Überwachung, Meldeanlagen und andere elektronische Vorrichtungen eingesetzt. Autorisiertes Personal erlangt über Multi-Faktor-Authentifizierungsmechanismen Zugang zu den Rechenzentren. Die Eingänge zu den Serverräumen sind mit Geräten abgesichert, die Alarm auslösen, wenn die Tür aufgebrochen oder offen gehalten wird

✓ **Regelmäßige Prüfung der Datenwiederherstellung**

im Rahmen des AVV

✓ **Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort**

✓ **In Hochwassergebieten: Serverräume über der Wassergrenze**

✓ **Klimaanlage in Serverräumen**

✓ **Schutzsteckdosenleisten in Serverräumen**

✓ **Feuerlöschgeräte in Serverräumen**

✓ **Backup- und Recoverykonzept**

Grundsätzlich greift das laufende System auf unterschiedliche Datenbanken zu. Die ununterbrochene Zurverfügungstellung und Leistung der Shore Lösung und ihrer Daten ist durch eine sog. Master-Slave-Replikation der Datenbanken gegeben. Bei einem Fehler (z.B. Stromausfall) in einer der Server/Datenbanken, kann ohne Verzögerung auf die gespiegelte Datenbank zugegriffen werden. Es werden täglich Backups der Daten erstellt. Welche verschlüsselt abgelegt sind. Unsere Backups reichen bis zu 15 Tage zurück. Dies bedeutet, dass im Falle einer Verletzung der Datensicherheit im laufenden System, die Daten dennoch wiederhergestellt werden können. Sowohl die Master-Datenbank und Slaven-Datenbank als auch die jeweiligen Backups sind voneinander getrennt. Erfolgt ein nicht autorisierter

Zugriff auf die Datenbanken, besteht kein Zugriff auf die Backups und andersrum. Außerdem liegen doppelte Backups der Daten vor.

- ✓ **Notfallplan zur Datenwiederherstellung**
- ✓ **Serverräume nicht unter sanitären Anlagen**

09. Trennungsgebot

Anforderung und Handhabung

- ✓ **Versehen der Datensätze mit Zweckattributen/Datenfeldern**
- ✓ **Festlegung von Datenbankrechten**
- ✓ **Logische Mandantentrennung (softwareseitig)**
- ✓ **Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden**

  Alle gespeicherten Daten werden nach dem Industriestandard AES verschlüsselt.
- ✓ **Trennung von Produktiv- und Testsystem**