GEWINN BLICK
Kassen- und Bezahlsysteme

Technische und organisatorische Maßnahmen zur Datensicherheit

Gewinnblick Allgäu-Oberschwaben GmbH
Mooswiesen 12, 88214 Ravensburg (Deutschland)

Version: 1.3

Stand: April 2023

Sehen, was wirklich zählt.

Bei der Gewinnblick Allgäu-Oberschwaben GmbH sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO getroffen worden:

1 Vertraulichkeit

1.1 Zutrittskontrolle

- Außentüren - Die Zugänge zum Bürohaus und auch zu den Büroräumen sind Tag und Nacht verschlossen.
- Besucherregelung - Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zu dem Bürohaus und dann den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.
- Home-Office - Es ist sichergestellt, dass erforderliche Sicherheitsmaßnahmen für Beschäftigte im Home-Office eingehalten werden.
- Server- und Netzwerkschränke (Racks) sind verschlossen und werden nur bei Wartungsarbeiten geöffnet. Die Schlüsselausgabe ist geregelt.
- Manuelles Schließsystem - Manuelles Schließsystem mit Schließzylinder
- Schließanlage - Einsatz einer Schließanlage
- Schlüsselverwaltung - Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

1.2 Zugangskontrolle

Für die Zugangskontrolle sind nachfolgende Maßnahmen von dem Verantwortlichen getroffen worden:

- Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von der Geschäftsführung freigegeben wurde.
- Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss.
- Remote-Zugriffe auf IT-Systeme erfolgen stets über verschlüsselte Verbindungen.
- Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.
- Alle Server sind durch Firewalls geschützt.
- Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet sind ebenfalls durch Firewalls gesichert.
- Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

1.3 Zugriffskontrolle

- Berechtigungen für IT-Systeme und Applikationen werden ausschließlich von Administratoren eingerichtet.
- Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen. Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten.
- Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.
- Die Vernichtung von Datenträgern und Papier erfolgt durch die Mitarbeiter, die eine Vernichtung nach DIN 66399 durchführen.
- Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.
- Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates durch einen externen EDV-Dienstleister aktualisiert.

1.4 Trennung

Alle vom Verantwortlichen für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet.

1.5 Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

2 Integrität

2.1 Eingabekontrolle

- Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die vom Verantwortlichen im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.
- Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

2.2 Weitergabekontrolle

- Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden erfolgt, darf jeweils nur in dem Umfang, wie erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.
- Alle Mitarbeiter, die in einem Kundenprojekt/Auftrag arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.
- Soweit möglich, werden Daten verschlüsselt an Empfänger übertragen.
- Die Nutzung von privaten Datenträgern ist den Beschäftigten im Zusammenhang mit Kundenprojekten untersagt.

- Mitarbeiter des Verantwortlichen werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

2.3 Verfügbarkeit und Belastbarkeit

- Daten auf Serversystemen werden regelmäßig gesichert.
- Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung, die im Falle einer Störung die Server kontrolliert herunterfährt.

2.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Es ist ein Datenschutzmanagement implementiert. Es gibt Richtlinien, mit denen die Umsetzung des Datenschutzes und der Datensicherheit gewährleistet wird.
- Es ist Datenschutz-Team (DST) eingerichtet, dass Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.
- Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.
- Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.
- Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.

2.5 Auftragskontrolle

- Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union.
- Es ist ein betrieblicher Datenschutzbeauftragter benannt. Stephan Krischke ist unter datenschutz@gewinnblick.de erreichbar.
- Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführtem Audit / Überprüfung durch den Datenschutzbeauftragten abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.