GEWINN BLICK
Kassen- und Bezahlsysteme

Technische und organisatorische Maßnahmen zur Datensicherheit

Gewinnblick Franken GmbH
Hertzstraße 2, 97076 Würzburg (Deutschland)

Version: 1.3

Stand: April 2023

Sehen, was wirklich zählt.

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

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der 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.
- IT-Schränke - 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.

M.1.2 Beschreibung der Zugangskontrolle:

- Abwesenheit Arbeitsplatz - Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Alternativ wird diese Maßnahme durch dementsprechende technische Maßnahmen umgesetzt
- Authentifikation mit Benutzer + Passwort - Authentifikation an den IT-Systemen mit Benutzername + Passwort
- Benutzerberechtigungen - Um Zugang zu IT-Systemen zu erhalten, müssen Benutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, durch Freigabe nach einem definierten Prozess (On- und Offboarding bzw. Abteilungswechsel).
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerkes. Das Regelwerk der Firewall beinhaltet eine Sperrung nicht benötigter Ports und Dienste.
- Internetzugriff - Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

- Monitoring - Auf den Servern der ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.
- Netzwerk-Segmentierung - Es besteht eine Netzwerksegmentierung und das interne Netzwerk bzw. WLAN ist vom Gäste-WLAN physisch oder per VLAN getrennt.
- Regelung zu mobilen Geräten - Mitarbeiter verpflichten sich zur Einhaltung der Vorgaben zur Verwendung dienstlicher Smartphones / Notebooks bzw. existiert eine BYOD-Regelung.
- Remote Access - Remote-Zugriffe auf IT-Systeme erfolgen stets über verschlüsselte Verbindungen
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren
- Verwaltung der Adminpasswörter - Administratorpasswörter werden zentral und verschlüsselt unter Verwendung eines Passworttools gespeichert. Der Leitung bzw. Geschäftsführung sind die Passwörter regelmäßig gesichert auszuhändigen.
- Zugang Serverraum - Der Zugang zum Serverraum ist über einen geregelten Prozess nur für einen bestimmten Personenkreis freigegeben
- Zugang zu Clouddiensten - Kritische interne IT-Systeme und cloudbasierte Anwendersoftware werden zusätzlich durch eine Zwei-Faktor-Authentifizierung gesichert.

M.1.3 Beschreibung der Zugriffskontrolle:

- Adminrechte - Berechtigungen für IT-Systeme und Applikationen werden ausschließlich von Administratoren eingerichtet.
- ADS, ERP etc. - 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.
- Berechtigungskonzept - Es besteht ein Berechtigungskonzept, dass Zugriffsberechtigungen und Passwortverfahren pro genutzter Anwendung und Dateisystem beschreibt. Ferner werden die Zugriffsrechte der Benutzer personen- oder rollenbasiert beschrieben.
- Datenlöschung - Sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben)
- Einsatz von Aktenvernichtern - Einsatz von Aktenvernichtern (min. Sicherheitsstufe 3 und Schutzklasse 2)
- IT-Infrastruktur physisch - Der physische Zugriff auf Server und zentrale Netzwerkkomponenten ist durch die Installation in IT-Schränken (Racks) abgesichert.

- On- und Offboarding - Es ist ein Verfahren etabliert, dass mit der Einstellung und dem Ausscheiden von Beschäftigten den Zugriff auf IT-Systeme berechtigt bzw. entzieht. Dieses Verfahren stellt sicher, dass inaktive Benutzer nach 6 Monaten deaktiviert werden.
- Passwortregelung 2020 - Es ist eine Passwortrichtlinie, die Länge (8 bis 15 Zeichen) und Komplexität (Buchstaben, Zahlen, Zeichen) technisch vorgibt, etabliert. Die Passwortstärke wird anhand des ermittelten Risikos (MFA verwendbar) und der technischen Möglichkeiten des jeweiligen IT-Systems festgelegt. Der Benutzer muss sein Initialpasswort mit der ersten Anmeldung wechseln und eine automatische Sperrung erfolgt bei wiederholter Falscheingabe. Benutzer führen Passwortwechsel periodisch durch, diese Maßnahme wird jährlich überprüft.
- Softwareinstallation - Den Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.
- Zentrale Benutzerverwaltung - 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. Zugriffsberechtigungen werden regelmäßig überprüft und bei Bedarf angepasst.

M.1.4 Beschreibung der Weitergabekontrolle:

- E-Mail-Verschlüsselung - E-Mail-Verschlüsselung mit S/MIME (Ende-zu Ende Verschlüsselung) oder TLS Verfahren (Transportverschlüsselung)
- Kundenprojekt - Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.
- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
- VPN-Tunnel - Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung - Die eingesetzten IT-System verfügen über eine logische Mandantentrennung (softwareseitig). Die Trennung von Daten von verschiedenen Kunden/Projekten ist stets gewährleistet.

M.1.7 Beschreibung der Verschlüsselung:

- Festplattenverschlüsselung - Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz.
- Serverzugriff - Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Benutzerkonten - Die Beschäftigten sind verpflichtet, stets mit ihren eigenen Benutzerkonten zu arbeiten. Benutzerkonten dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.
- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung Dateisystem - Protokollierung der Eingabe, Änderung und Löschung von Daten auf Dateisystemen.
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Aktualisierung von Anwendersoftware - Es ist ein Verfahren etabliert, dass die regelmäßige Aktualisierung der Standard- und Individualsoftware sicherstellt. Dieses Verfahren beinhaltet automatisierte Verfahren mit zentraler Steuerung, als auch manuelle Prozesse, die je nach technischer Vorrausetzung der Anwendersoftware geplant werden.
- Backup- & Recoverykonzept - Es existiert ein Backup- & Recoverykonzept, das täglich überprüft wird.
- Datensicherungskonzept - Das Datensicherungskonzept beinhaltet die Anforderungen der "3-2-1-0" Regelung, wie folgt:
  3 = Zu den primären Daten werden an zwei weiteren Sicherungsdateien gespeichert;
  2 = Eine der Sicherungskopien ist auf einem internen Medium (NAS) und die andere Kopie auf einem Wechselspeichermedium (Cloud-Speicher) gesichert.
  1 = Mindestens eine Sicherungskopie ist nicht vor Ort vorgehalten, an dem sich die Primärdaten und die Primärsicherung befindet.
  0 = Das Backup wird täglich überwacht und ist gegen Schadcode abgesichert, um Fehler zu finden, um diese so schnell wie möglich zu beheben. Zweitens ist sichergestellt, dass die Daten aus dem Backup wiederherstellbar sind, indem in regelmäßigen Abständen Wiederherstellungstests stattfinden.
- Monitoring - Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.
- Patchmanagement - Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits- und Software-Updates aktualisiert.
- Unterbrechungsfreie Stromversorgung - (USV) Unterbrechungsfreie Stromversorgung

- Viren- und Malwareschutz - Einsatz einer mehrstufigen Absicherung gegenüber Viren und Malware. Es ist gewährleistet, dass die Absicherung der IT-Systeme tagesaktuell ist und der Status in regelmäßigen Abständen überwacht wird.

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Datenwiederherstellungen - Regelmäßige und dokumentierte Notfalltests zur Wiederherstellung der IT-Systeme (Notfallübung).
- Incidentmanagement - Es besteht ein Verfahren (bspw. nach ITIL Standard), dass zwischen Ausfällen / Störungen und Sicherheitsvorfällen unterscheidet. Meldungen werden zentral in einem Ticketsystem protokolliert und die Bearbeitung dokumentiert. In regelmäßigen Abständen werden Vorfälle ausgewertet, um Schwachstellen in IT-Systemen proaktiv entgegenzuwirken.

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Audits - Regelmäßige Datenschutzaudits der beauftragten Dienstleister durch den Datenschutzbeauftragten
- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit und Subdienstleister)
- Datenverarbeitung - Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union oder im Europäischen Wirtschaftsraum.
- Dienstleister - Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts eine angemessene Datenschutzregelung getroffen. Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO.
- DSB - Benennung eines externen Datenschutzbeauftragten: Stephan Krischke, erreichbar unter datenschutz@gewinnblick.de
- Laufende Überprüfung - Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.
- Verpflichtung - Verpflichtung der Dienstleister auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- Audits - Durchführung regelmäßiger interner Audits zur Wirksamkeitskontrolle der durchgeführten Maßnahmen.
- DSMS - Im Unternehmen ist ein Datenschutzmanagementsystem (DSMS) implementiert. Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.
- DST - Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.
- Incident-Response-System - 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.
- Meldung Aufsichtsbehörde - 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.
- Regelungen zum Datenschutz und der IT-Sicherheit - Es bestehen schriftliche Regelungen zum Datenschutz und Datensicherheit (Arbeitsvertrag, Datenschutzhandbuch). Beschäftigte werden auf die Einhaltung der dieser Regelungen geschult und verpflichtet.
- Schulungskonzept - Es ist ein Schulungskonzept etabliert, dass regelmäßige an Gefahren und Bedrohungen ausgerichtete Schulungen durchführt. Es ist mit der Einstellung neuer Beschäftigter sichergestellt, dass diese eine Einweisungsschulung erhalten.
- Schwachstellenanalysen - Durchführung regelmäßiger interner Datensicherheitsaudits (mind. jährlich) unter Verwendung eines automatisierten Schwachstellenscans mit anschließender Bewertung und Aktualisierung der technisch-organisatorischen Maßnahmen
- Verpflichtung der Beschäftigten - Beschäftigte werden zur Vertraulichkeit im Umgang mit personenbezogenen Daten sowie der Verschwiegenheit gegenüber dem Geschäftsgeheimnis verpflichtet. Diese Verpflichtung beinhaltet auch die Nutzung sozialer Medien.