Datensicherheitskonzept der Staatanzeiger für Baden-Württemberg GmbH & Co. KG

Zutrittskontrolle

1. Unbefugte werden durch Schlüsselvergabe (RFID) daran gehindert, die Räume des Unternehmens zu betreten und damit an die Datenverarbeitungsanlagen zu gelangen. Die Schlüssel werden nach Funktion und Verantwortungsbereich getrennt vergeben. Die Schlüsselvergabe wird dokumentiert.
2. Besucher dürfen sich nur unter Aufsicht innerhalb der Firmenräumlichkeiten aufhalten.
3. Es existiert eine Alarmanlage.
4. Die Haupttüren sind durch ein Zeitschloss zusätzlich abgesichert.

Zugangskontrolle

1. Der Zugang zum Arbeitsplatzrechner wird durch Passwörter geregelt. Die Mitarbeiter müssen in regelmäßigen Abständen ihr Passwort zu wechseln. Für das Passwort ist eine Länge von mindestens 8 Zeichen und eine Kombination aus Buchstaben und Zahlen erforderlich. Zugangskennungen und Passwörter dürfen nicht an Dritte weitergegeben werden. Der Arbeitsplatz wird nach einer definierten Anzahl von fehlgeschlagenen Zugriffsversuchen gesperrt.
2. Nutzer von Anwendungssoftware müssen sich unter Angabe von Benutzerkennung und mit Passwort am System anmelden. Alle Benutzer werden zentral verwaltet. Nur der Administrator hat Zugang zur Benutzerverwaltung. Dort werden die verschiedenen Berechtigungen erstellt und Mitarbeitern zugeteilt.

Zugriffskontrolle

1. Bei kritischen Zugriffen kommen Virtual Private Networks (VPN) zum Einsatz.
2. In der Dateiverwaltung wird das Lesen, Kopieren, Ändern oder Löschen von Daten seitens nicht autorisierter Personen durch Benutzerkonten mit unterschiedlichen Rechten verhindert.
3. Sämtliche Zugriffe sowie von Missbrauchsversuche werden protokolliert. Die Protokolle werden durch den DSB kontrolliert.
4. Papierausdrucke mit personenbezogenen Daten werden in speziellen Behältern gesammelt und durch einen zertifizierten Entsorgungsbetrieb rückinformationssicher vernichtet. Zusätzlich existieren mobile Aktenvernichter der Stufe P4.

Weitergabekontrolle

1. Personenbezogene Daten werden in der Datenbank gespeichert und grundsätzlich nur an auftragsbezogene Mitarbeiter/innen weitergegeben.
2. Der Datenaustausch mit Kunden kann bei Bedarf verschlüsselt oder passwortgeschützt erfolgen.
3. Daten, die von Kundenseite zur Verfügung gestellt werden, werden ausschließlich auf eigenen Systemen bearbeitet. Im Bedarfsfall erstellte Sicherheitskopien werden nach erfolgreichem Abschluss der Bearbeitung gelöscht.

Eingabekontrolle

Die Erstellung, Änderung und Entfernung von sensiblen Daten in der Datenbank werden protokolliert.

Auftragskontrolle

Bei der Verarbeitung von personenbezogenen Daten im Rahmen einer Auftragsdatenverarbeitung wird sichergestellt, dass die Datenverarbeitung auf Weisung des Kunden und nur im Rahmen dieser Weisungen stattfindet. Eine darüber hinausgehende unbefugte Datenverarbeitung ist den Mitarbeiter/innen vertraglich durch eine schriftliche Datenschutzvereinbarung untersagt. Der Inhalt der Weisungen eines Kunden wird den mit der Bearbeitung des jeweiligen Auftrags betrauten Mitarbeiter/innen verbindlich mitgeteilt. Alle Mitarbeiter die mit der Bearbeitung der Daten betraut sind wurden nach §5 BDSG auf den Datenschutz verpflichtet. Mit externen Auftragnehmern, die personenbezogene Daten im Auftrag verarbeiten, sind Datenschutzvereinbarungen nach § 11 BDSG abgeschlossen worden.

Verfügbarkeitskontrolle

1. Alle Arbeitsplatzrechner sind durch eine Firewall vor Angriffen von außen geschützt. Alle Rechner werden durch entsprechende Software vor Schadprogrammen und Viren geschützt.
2. Alle Daten, die in einer Datenbank gespeichert sind, werden durch täglich erstellte Backups gesichert. Die erstellte Sicherungskopie wird in einem anderen Brandabschnitt gelagert. Die Rücksicherung der Daten wird regelmäßig überprüft.
3. Es existieren 2 redundante Server. Die Server sind durch eine Unterbrechungsfreie Stromversorgung (USV) vor Ausfall geschützt. Eine Brandmeldeanlage ist vorhanden.

Trennungskontrolle

Daten, die einer Trennpflicht unterliegen, werden logisch getrennt voneinander auf den Servern gespeichert und verarbeitet.

Organisationskontrolle

1. Ein externer Datenschutzbeauftragter mit Nachweis der nötigen Fachkunde wurde schriftlich bestellt.
2. Das öffentliche Verfahrensverzeichnis liegt vor und kann auf Anfrage zur Verfügung gestellt werden.
3. Die Mitarbeiter werden regelmäßig auf den Datenschutz sensibilisiert und geschult.