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

Sicherheit der Verarbeitung / Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

1. Maßnahmen zur Sicherstellung von Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

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

Zugangskontrolle

1. Der Zugang zum Arbeitsplatzrechner wird durch Passwörter geregelt.
2. Alle Benutzer werden zentral verwaltet.
   Nur der Administrator hat Zugang zur Benutzerverwaltung. Dort werden die verschiedenen Berechtigungen erstellt und Mitarbeitern zugeteilt.
3. Nutzer von Anwendungssoftware müssen sich unter Angabe von Benutzerkennung und mit Passwort an dem System anmelden.
4. Die Mitarbeiter sind gezwungen, in regelmäßigen Abständen ihr Passwort zu wechseln. Dabei muss eine Länge von mindestens 8 Zeichen und eine Kombination aus Buchstaben, Zahlen eingehalten werden.

Zugriffskontrolle

1. In der Dateiverwaltung wird das Lesen, Kopieren, Ändern oder Löschen von

Daten seitens nicht autorisierter Personen durch Benutzerkonten mit unterschiedlichen Rechten verhindert.

2. Virtual Private Networks (VPN) kommen bei kritischen Zugriffen zum Einsatz.
3. Automatisches log-off (VPN) bei Inaktivität nach einer bestimmten Zeit.
4. Protokollierung der Zugriffe sowie von Missbrauchsversuchen. Die Protokolle werden durch den DSB kontrolliert.
5. Papierausdrucke mit personenbezogenen Daten werden in speziellen Behältern gesammelt und durch einen zertifizierten Entsorgungsbetrieb rückinformationssicher vernichtet. Zusätzlich existieren mobile Aktenvernichter der Stufe P4.

Trennungskontrolle

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

Pseudonymisierung

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Maßnahmen zur Sicherstellung von Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

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 Passwort geschützt 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

Das Erstellen, die Änderung und das Entfernen von sensiblen Daten in der Datenbank werden protokolliert.

3. Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

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

4. Maßnahmen zur Sicherstellung der Belastbarkeit

Die technischen und organisatorischen Maßnahmen werden regelmäßig vom Datenschutzbeauftragten überprüft.

5. Maßnahmen zur Gewährleistung der Wirksamkeitskontrolle

Die technischen und organisatorischen Maßnahmen werden regelmäßig vom Datenschutzbeauftragten überprüft.

6. „Weisungskontrolle/Auftragskontrolle“ - eindeutige Vertragsgestaltung

Mit Unterauftragnehmern werden Vereinbarungen zur Auftragsdatenverarbeitung gem. Art. 28 Abs. 3 DSGVO abgeschlossen. Diese regeln unter anderem:
- die Rechte und Pflichten des Auftragsverarbeiters und des Verantwortlichen
- Prozess zur Erteilung und/oder Befolgung von Weisungen
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- Unabhängige Auditierung der Weisungsgebundenheit
- Verpflichtung der Mitarbeiter zur Vertraulichkeit