Technisch und Organisatorische Maßnahmen der KIV Thüringen GmbH (TOMs)

Zutrittskontrolle

Es wird ein mehrstufiges geschütztes Zutrittskontrollsystem mit entsprechender Überwachungs- und Einbruchsschutz eingesetzt. Die Verwaltung von Schlüsseln, Ident-Karten oder Transpondern erfolgt dokumentiert in Rahmen eines Antragsverfahren. Zur Überwachung datenverarbeitender Anlage gelten besondere Richtlinien und Bestimmungen zur Dokumentation, Überwachung des Zutrittsschutzes für einen eingeschränkten Personenkreis.

Zugangskontrolle

Es erfolgt ein mehrstufig, geschützter Zugang zu datenverarbeitenden Systemen. Hierbei werden über entsprechend dokumentierte Antragsverfahren an die innerhalb der datenverarbeitenden Stelle tätigen Personen Benutzerkennungen und Passwörter erteilt, deren Sicherheit und Komplexität über entsprechende Vorgaben innerhalb der eingesetzten Systeme, sichergestellt werden. Hierzu zählen u. a. Mehrfaktorauthentifizierung, Sitzungskontrolle und verschlüsselter Austausch von Anmelde- und Berechtigungsinformationen.

Zugriffskontrolle

Über differenzierte Berechtigungen (Profile, Rollen, Transaktionsrechte) agieren Datenverarbeiter innerhalb der eingesetzten Systeme voneinander isoliert. Der Datenverarbeiter ist jederzeit durch seine personifizierte ihm zuordenbare Benutzerkennung ermittelbar.

Über entsprechende technische Einrichtungen, können die durch den Datenverarbeiter ausgeführten Transaktionen, auf den zur Auftragserfüllung überlassenen Daten nachgewiesen werden und überwachte werden.

Hierzu zählen die ordnungsgemäße Verwendung der Daten, insbesondere bei der Durchführung von Erhebungen Veränderungen, Veränderung und Löschung von den zur Auftragserfüllung notwendigen Daten.

Die unberechtigte Datennutzung durch Dritte wird durch regelmäßige Kontrolle der Datenverwendung durch den Verantwortlichen der Datenverarbeitenden Stelle, den für die Verarbeitung beauftragte Stelle, sowie den benannten Datenschutzbeauftragten überprüft und überwacht.

Weitergabekontrolle

Werden im Rahmen der Datenverarbeitung Daten an Dritte übermittelt, so wird deren Übertragung, Speicherung und Transport durch entsprechende technische Einrichtungen nach aktuellem Stand der Technik sichergestellt. Hierfür werden die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verwandt.

Eingabekontrolle

Über alle Aktivitäten des Datenverarbeiters und der dafür genutzten technischen Einrichtungen zur Verarbeitung, Speicherung und Übermittlung sowie das hierbei wirkende Organisationssystem werden Protokolle geführt.

Auftragskontrolle

Die Verarbeitung der Daten innerhalb der technischen Einrichtungen der KIV Thüringen GmbH oder deren Übermittlung an Dritte erfolgt generell auf entsprechender Rechtsgrundlagen.

Die für die Datenverarbeitung unterstützenden Dritte, wie z.B. technische Dienstleister sind generell vertraglich zur Einhaltung der bestehenden Rechtsgrundlage wie Datenschutzgrundverordnung (DSGVO), Bundesdatenschutzgesetz (BDSG) und Landesdatenschutzgesetze (LDSG) verpflichtet.

Die Kontrolle der technisch angemessenen und ordnungsgemäßen Verarbeitung der Datenverarbeitung obliegt der verantwortlichen Datenverarbeitenden Stelle, vertreten durch den bestellten IT-Sicherheitsbeauftragten der KIV Thüringen GmbH.

Verfügbarkeitskontrolle

Zur Sicherstellung und Überwachung der Grundsätze der sicheren Datenverarbeitung wie Verfügbarkeit, Integrität und Vertraulich werden in der KIV Thüringen GmbH umfangreiche technische Maßnahmen ergriffen. Hierzu gehören unter anderem die Bereitstellung von Redundanzen für die Speicherung, der Verarbeitung und den Transport von Daten, Antivirenschutz, unterbrechungsfreie Stromversorgungen und Netzwerkmanagementsysteme.

Über entsprechende technische Einrichtungen werden die zur Verarbeitung überlassenen Daten vor Verlust geschützt. Im Rahmen des Schutzes der Daten, werden diese in Form von Backup-Sätzen außerhalb der Geschäftsräume gelagert. Hierbei werden diese Backup-Sätze verschlüsselt und in geeigneter Form verwahrt (z.B. Bankschließfach etc.).

Über ein entsprechendes Eskalationsmanagement, werden bei Verstoß gegen Grundsätze der Datenverarbeitung Maßnahmen zur Eindämmung und Minderung des Schadensausmaßes und zur Wiederaufnahme nach Ausfällen bearbeitet. Entsprechende Notfallpläne und Meldungen an die gesetzlich vorgeschriebenen Stellen werden in diesem Rahmen durchgeführt.

Trennungskontrolle

Zur Einhaltung des Trennungsgebotes werden umfängliche technische Maßnahmen zur Trennung und Verwahrung der Daten während des Transports, der Speicherung und Verarbeitung getroffen. Hierzu zählen u. A. der Einsatz getrennter Netzwerke, dedizierter Adressbereiche, Mandantentrennung und Firewalls.

Technischer Fortschritt

Änderung gemäß dem technischen Fortschritt und der Erhöhung des Datenschutzes sind vorbehalten.