TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN GEMÄSS ART. 32 DSGVO

SYSTOPIA GmbH
Adenauerallee 12-14
53113 Bonn

Letzte Aktualisierung: 5.2.2026

Die Auswahl und Ausgestaltung der technischen und organisatorischen Maßnahmen erfolgt unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig überprüft und bei Bedarf an veränderte rechtliche, technische oder organisatorische Rahmenbedingungen angepasst. Die Maßnahmen werden dokumentiert und sind Bestandteil des internen Datenschutz- und Informationssicherheitsmanagements.

ZUTRITTSKONTROLLE

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Regelung und Dokumentation von Zutrittsberechtigungen für Mitarbeitende und externe Personen
- Begleitung und Kontrolle von Besuchern in sensiblen Bereichen
- Schlüsselregelung (Schlüsselausgabe etc.)
- Manuelles Schließsystem
- Sicherheitsschlösser

ZUGANGSKONTROLLE

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Schlüsselregelung (Schlüsselausgabe etc.)
- Erstellen von Benutzerprofilen
- Einsatz von VPN-Technologie
- Sicherheitsschlösserzusenden

- Regelmäßige Überprüfung und Aktualisierung von Benutzerkonten
- Unverzügliche Deaktivierung von Zugängen bei Rollenwechsel oder Ausscheiden von Mitarbeitenden

ZUGRIFFSKONTROLLE

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und Speicherung vor unbefugtem Zugriff, Veränderung oder Verlust geschützt sind.

- Verwaltung von Zugriffs- und Berechtigungsrechten nach dem Need-to-know-Prinzip
- Beschränkung administrativer Berechtigungen auf das erforderliche Mindestmaß
- Etablierung und Durchsetzung einer Passwort- und Authentifizierungsrichtlinie, die den jeweils aktuellen anerkannten Standards (insbesondere BSI-Empfehlungen) entspricht
- Einsatz geeigneter Verfahren zur sicheren Erstellung, Nutzung und Verwaltung von Zugangsdaten
- Verwendung zeitgemäßer Verschlüsselungsverfahren zum Schutz personenbezogener Daten auf Datenträgern und in IT-Systemen
- Einsatz geeigneter Aktenvernichtungs- und Datenträgervernichtungsverfahren nach dem Stand der Technik
- Regelmäßige Überprüfung und Anpassung von Berechtigungen
- Protokollierung sicherheitsrelevanter Zugriffe im Rahmen der gesetzlichen und betrieblichen Erfordernisse
- Schulung der Mitarbeitenden zu sicheren Zugriffs- und Authentifizierungsverfahren

WEITERGABEKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Absicherung elektronischer Kommunikationswege durch geeignete kryptographische Verfahren nach dem Stand der Technik
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- E-Mail-Verschlüsselung
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Dokumentation und Kontrolle von Datenübermittlungen an interne und externe Empfänger

EINGABEKONTROLLE

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines

Berechtigungskonzepts

- Regelmäßige Auswertung von Protokolldaten zur Erkennung unbefugter oder ungewöhnlicher Zugriffe
- Schutz der Protokolldaten vor Manipulation und unbefugtem Zugriff

AUFTRAGSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO nur auf entsprechende Weisung des Auftraggebers, basierend insbesondere auf eindeutiger Vertragsgestaltung, formalisiertem Auftragsmanagement, strenger Auswahl des Dienstleisters und Kontrollen

RASCHE WIEDERHERSTELLBARKEIT

- Erstellen eines Backup- und Recoverykonzepts
- Testen von Backups und Datenwiederherstellung

VERFÜGBARKEITSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Testen von Datenwiederherstellung
- Erstellen, Umsetzen und Testen eines Backup- & Recoverykonzepts

TRENNUNGSGEBOT

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Sicherstellung der Zweckbindung durch technische und organisatorische Trennung von Datenverarbeitungen mit unterschiedlichen Verarbeitungszwecken
- Technische und organisatorische Maßnahmen zur Vermeidung unzulässiger Zweckänderungen
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Trennung von Produktiv- und Testsystem
- Festlegung von Datenbankrechten

Diese technischen und organisatorischen Maßnahmen werden regelmäßig überprüft, fortgeschrieben und an neue rechtliche, technische und organisatorische Anforderungen angepasst.