Technische und Organisatorische Maßnahmen gemäß Art. 32 Datenschutzgrundverordnung

Sowohl die Datenschutzgrundverordnung wie auch das Bundesdatenschutzgesetz regeln Anforderungen an die Sicherheit der personenbezogenen Daten. Danach haben sowohl der Verantwortliche als auch der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter geeignete technische und organisatorische Maßnahmen zum Schutz der Daten zu ergreifen. Hier aufgeführt sind die technischen und organisatorischen Maßnahmen des **Auftragsverarbeiters**.

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen …

- Alarmanlage mit Aufschaltung auf ein Sicherheitsunternehmen
- Regelung für die Vergabe von Zutrittsberechtigungen
- Elektronisches Zugangskontrollsystem
- Für die Mitarbeiter gelten abgestufte Zutrittsregelungen
- Besucher dürfen nur in Begleitung von berechtigten Mitarbeitern in die Sicherheitsbereiche eintreten
- Protokollierung der Besucher
- Wartungstechniker arbeiten grundsätzlich unter Aufsicht
- Reinigung der Sicherheitsbereiche erfolgt unter Aufsicht

Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern …

- Funktions- und Rollenkonzept
- Userbezogene Passwortvergabe
- Passwortrichtlinien (Mindestens 8 Zeichen, Kombination aus Buchstaben, Sonderzeichen, Ziffern, sowie die Nutzung von Groß- und Kleinschreibung)
- Externer Zugang für Mitarbeiter nur über gesicherte und verschlüsselte VPN-Anbindung
- Regelmäßiger Passwortwechsel
- Identifikation und Authentifikation von Benutzern
- Sperrung bei Fehlversuchen

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing …

- Trennung von Produktiv- und Testsystemen
- Berechtigungskonzept

Pseudonymisierung

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 …

———————

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur …

- Festgelegte Wege und Verfahren der Übermittlung
- Abgesicherte Übermittlung
- Sichere Datenübertragung zwischen Server und Clients
- Verschlüsselte Ablage von Daten auf der Festplatte

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement …

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Aufbewahrungsfristen für Revision und Nachweiszwecke

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne …

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in den Serverräumen
- Virenschutz
- Firewalls
- Lizenzüberwachung
- Brandschutzeinrichtungen, Rauchverbot
- Regelmäßige Datensicherung, Backup-Konzept
- Plan für zu ergreifende Sofortmaßnahmen bei einem Notfall

Wiederherstellungskontrolle

Wie wird gewährleistet, dass die Systeme und Daten nach einem Störungsfall wiederhergestellt werden?

- Sowohl MDS als auch die eingesetzten Druckdienstleister besitzen Backup-Konzepte, für die Wiederherstellung im unwahrscheinlichen Fall eines Systemkomplettausfalls.

Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen …

- Regelungen der Zuständigkeiten und Verantwortlichkeiten
- Auswahl der Auftragnehmer unter Sorgfaltsgesichtspunkten
- Dokumentation aller Aufträge

Betriebsorganisation und Rechenschaftspflicht

Durch welche Maßnahmen ist die innerbetriebliche Organisation so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird?

- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
- Datenschutzmanagement
- Maßnahmen zur Planung, Organisation, Steuerung und Kontrolle der gesetzlichen und betrieblichen Anforderungen des Datenschutzes durch die Bestellung eines externen Datenschutzbeauftragten mit der Sicherstellung regelmäßiger Überprüfungen und Anpassungen der Datenschutzorganisation.
- Incident-Response-Management
- Maßnahmen zur Reaktion auf erkannte und vermutete Sicherheitsvorfälle und Störungen mit festgelegten internen und externen Kommunikations- und Eskalationsprozesse
- Datenschutzfreundliche Voreinstellungen
- Maßnahmen zur Berücksichtigung datenschutzrelevanter Belange werden bereits während der Entwicklung eines Prozesses so getroffen, dass Systeme und Anwendungen des Auftragnehmers vor der Verwendung sicher konfiguriert und voreingestellt („privacy by default") werden. Standardeinstellungen der Produkte werden vor der ersten Verwendung überprüft und sicher angepasst.

Unsere technischen und organisatorischen Maßnahmen (TOM) sind jederzeit einzusehen unter: https://www.mds-it.de/datenschutz.html

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Über Richtlinien, Arbeitsanweisungen und Sicherheitskonzepte werden die organisatorischen Maßnahmen geprüft
- Regelmäßige Kontrollen, Dokumentation und ggf. Optimierung werden für die technischen Maßnahmen durchgeführt