Technisch-Organisatorische Maßnahmen

TOM KMU Tools V3

KMU Tools e. K.
Martin Kramer (Inhaber)
Remscheider Str. 4
28844 Weyhe
Deutschland
Telefon: 0421-98977775
Fax: 0421-98985285
E-Mail: office@kmu-tools.de

Inhaltsverzeichnis

1 Einleitung und Rahmenbedingungen

1.1 Einleitung

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1.2 Unternehmen / Behörde

Die folgenden Festlegungen repräsentieren das Datenschutzkonzept der

KMU Tools e. K.
Martin Kramer (Inhaber)
Remscheider Str. 4
28844 Weyhe
Deutschland
Telefon: 0421-98977775
Fax: 0421-98985285
E-Mail: office@kmu-tools.de

1.3 Mit dem Datenschutz beauftragte Person des Unternehmens / der Behörde

KMU Tools e. K.
Martin Kramer (Inhaber)
Remscheider Str. 4
28844 Weyhe
Deutschland
Telefon: 0421-98977775
Fax: 0421-98985285
E-Mail: m.kramer@kmu-tools.de

2 Technisch-Organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen Folgendes ein:

2.1 Gewährleistung der Vertraulichkeit

2.1.1 Zutrittskontrolle

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

Maßnahmen:

- Besucher nur in Begleitung durch Mitarbeiter
- Empfang ohne Rezeption
- Überwachter Eingangsbereich

2.1.2 Zugangskontrolle

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

Maßnahmen:

- Allgemeine Richtlinie Datenschutz und / oder Sicherheit
- Anti-Viren-Software
- Anti-Virus-Clients
- Anti-Virus-Software für mobile Geräte
- Anwendung einer 2-Faktor-Authentifikation
- Automatische Desktopsperre
- Einsatz von VPN bei Remote-Zugriff
- Erstellen von Benutzerprofilen
- Firewall
- Richtlinie „Sicheres Passwort“
- Verschlüsselung von Datenträgern
- Zugangssperre bei mehr als 3 Anmeldeversuchen

2.1.3 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 nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen:

- Auslagerung von Sicherungsdatenträgern
- Datenschutztresor
- Einsatz der minimalen Anzahl an Administratoren
- Festlegungen zur Datenträgerverwendung
- Manuelle Protokollauswertung
- Protokollierung der Aussonderung von Datenträgern
- Shell-Zugriff
- Verwaltung der Benutzerrechte durch Administratoren

2.1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Maßnahmen:

- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testumgebung

2.2 Gewährleistung der Integrität

2.2.1 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.

Maßnahmen:

- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Einsatz von VPN-Technologie
- Email-Verschlüsselung

2.2.2 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.

Maßnahmen:

- Klare Zuständigkeiten für die Löschung von Daten
- Nachvollziehbarkeit der Bearbeitung von Daten durch individuelle Benutzernamen
- Technische Protokollierung der Änderung von Daten
- Technische Protokollierung der Eingabe von Daten
- Technische Protokollierung der Löschung von Daten
- Vergabe von Rechten zur Bearbeitung von Daten

2.3 Pseudonymisierung und Verschlüsselung

2.3.1 Pseudonymisierung

Maßnahmen, die eine Pseudonymisierung von Daten gewährleisten.

Maßnahmen:

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe zu pseudonymisieren
- Interne Anweisung, personenbezogene Daten nach Ablauf der Löschfrist zu pseudonymisieren

2.3.2 Verschlüsselung

Maßnahmen, die eine Verschlüsselung von Daten gewährleisten.

Maßnahmen:

- Verschlüsselter Zugriff auf Datenbanken von Kunden
- Verschlüsselter Zugriff auf Server von Kunden
- Verschlüsselung des Transports von E-Mails

2.4 Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

2.4.1 Verfügbarkeit (der Daten)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Verfügbarkeit von Daten.

Maßnahmen:

- Backup & Recovery-Konzept
- Betrieb von Hochverfügbarkeits-Webservern
- Datensicherungskonzept vorhanden
- Kontrolle des Sicherungsvorgangs
- Monatliche Backups
- RAID System / Festplattenspiegelung
- SLA mit Hosting Dienstleister
- Tägliche Backups
- Unterbrechungsfreie Stromversorgung (USV)
- Wöchentliche Backups

2.4.2 Belastbarkeit (der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Belastbarkeit der Systeme.

Maßnahmen:

- Einsatz von Software Firewalls
- Einspielen von aktuellen Sicherheitsupdates auf allen Applikationsservern
- Einspielen von Sicherheitsupdates auf allen Entwicklersystemen

2.4.3 Wiederherstellbarkeit (der Daten / der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Wiederherstellbarkeit von Daten und Systemen.

Maßnahmen:

- Keine Maßnahmen

2.5 Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

2.5.1 Auftragskontrolle

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

Maßnahmen:

- Abschluss der notwendigen Auftragsdatenvereinbarungen
- Abschluss der notwendigen Standard-Vertragsklauseln
- Regelung zum Einsatz von Subunternehmern
- Sicherstellung der Vernichtung von Daten nach Beendigung eines Auftrags
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen / Dokumentation

2.5.2 Datenschutz-Management

Maßnahmen, die gewährleisten, dass Methoden evaluiert wurden, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, organisieren, steuern und kontrollieren.

Maßnahmen:

- Bestellung eines internen Datenschutzbeauftragten
- Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- Durchführung von Datenschutzfolgeabschätzungen (bei Bedarf)
- Einhaltung der Informationspflichten gemäß Art. 13 DSGVO
- Einhaltung der Informationspflichten gemäß Art. 14 DSGVO
- Einsatz von Softwarelösungen für Datenschutz-Management
- Regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz
- Schulung der Mitarbeiter zum Datenschutz
- Überprüfung der Wirksamkeit der TOMs (mind. jährlich durchgeführt)

2.5.3 Incident-Response-Management

Maßnahmen, die gewährleisten, dass Sicherheitsvorfällen vorgebeugt werden kann oder im Falle von bereits eingetretenen Sicherheitsvorfällen, dass Daten und Systeme geschützt werden können und eine schnelle Analyse und Behebung des Sicherheitsvorfalls durchgeführt werden kann.

Maßnahmen:

- Dokumentation von Sicherheitsvorfällen
- Einbindung von Datenschutzbeauftragten in Sicherheitsvorfälle
- Einsatz von Firewall und deren regelmäßige Aktualisierung
- Einsatz von Spamfilter und deren regelmäßige Aktualisierung
- Einsatz von Virenscanner und deren regelmäßige Aktualisierung

2.5.4 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass bereits durch die entsprechende Technikgestaltung (privacy by design) und Werkseinstellungen (privacy by default) einer Software vorab ein gewisses Datenschutzniveau herrscht.

Maßnahmen:

- Gewährleistung einer einfachen Ausübung des Widerrufsrechts eines Betroffenen
- Personenbezogene Daten werden nur zweckerforderlich erhoben