

Hinweise für die Erstellung der Anlage TOM (BMW Motoren GmbH)

„Übersicht technische und organisatorische Maßnahmen“

**zur Zusatzvereinbarung über eine Datenverarbeitung im Auftrag (DViA) nach
§ 10 DSGVO**

Technische und organisatorische Maßnahmen nach § 14 DSGVO und dessen Anlage:

1. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

Beispiele

- ⇒ Zutrittskontrollsystem,
Ausweisleser, Magnetkarte, Chipkarte
- ⇒ Schlüssel / Schlüsselvergabe
- ⇒ Türsicherung (elektrische Türöffner usw.)
- ⇒ Werkschutz, Pförtner
- ⇒ Überwachungseinrichtung
Alarmanlage, Video- / Fernsehmonitor

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Beispiele

- ⇒ Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- ⇒ Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- ⇒ Einrichtung eines Benutzerstammsatzes pro User
- ⇒ Verschlüsselung von Datenträgern

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Beispiele

- ⇒ Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- ⇒ Auswertungen
- ⇒ Kenntnisnahme
- ⇒ Veränderung
- ⇒ Löschung

4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle...

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Beispiele

- ⇒ Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
- ⇒ Elektronische Signatur
- ⇒ Protokollierung
- ⇒ Transportsicherung

5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Beispiel

- ⇒ Protokollierungs- und Protokollauswertungssysteme

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

Beispiele

- ⇒ Eindeutige Vertragsgestaltung
- ⇒ Formalisierte Auftragserteilung (Auftragsformular)
- ⇒ Kriterien zur Auswahl des Auftragnehmers
- ⇒ Kontrolle der Vertragsausführung

7. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch / logisch):

Beispiele

- ⇒ Backup-Verfahren
- ⇒ Spiegeln von Festplatten, z.B. RAID-Verfahren
- ⇒ Unterbrechungsfreie Stromversorgung (USV)
- ⇒ Getrennte Aufbewahrung
- ⇒ Virenschutz / Firewall
- ⇒ Notfallplan

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Beispiele

- ⇒ "Interne Mandantenfähigkeit" / Zweckbindung
- ⇒ Funktionstrennung / Produktion / Test)