Im Einzelnen werden folgende Maßnahmen bestimmt (Art. 32 Abs. 1 lit b.DSGVO):

1. Zugangskontrolle zu den Räumlichkeiten und Einrichtungen

Unbefugter Zugang (im physikalischen Sinn) muss verhindert werden. Technische und organisatorische Maßnahmen, um den Zugang zu den Räumlichkeiten und Einrichtungen zu kontrollieren, insbesondere um die Autorisierung zu prüfen:

- Zutrittskontrollsystem mit
- ID-Lesegerät, Magnetkarte, Chipkarte
- Protokollierung Vergabe von Schlüsseln
- Sicherheitspersonal
- Überwachungseinrichtungen,
- Video-/ CCTV-Bildschirme

2. Kontrolle des Zugriffs auf Systeme

Unbefugter Zugriff auf IT-Systeme muss verhindert werden. Technische (ID-/Kennwortsicherheit) und organisatorische (Benutzer-Stammdaten) Maßnahmen zur Identifizierung und Authentisierung des Benutzers:

- Kennwortverfahren (inkl. Sonderzeichen, minimale Länge, Ändern des Kennworts)
- Automatische Blockierung (z. B. Kennwort oder Timeout)
- Verschlüsselung
- 2-Faktoren Authentifizierung

3. Kontrolle des Zugriffs auf Daten

Nicht durch die zugewiesenen Zugriffsrechte gedeckte Aktivitäten in IT-Systemen sind zu vermeiden. Anforderungsbasierte Definition der Genehmigungsregelung und Zugriffsrechte, sowie Überwachung und Protokollierung der Zugriffe:

- Differenzierte Zugriffsrechte (über verschiedene Rollen)
- Berichte über Zugriffe
- Änderungen verfolgen nach Zugriffen pro user
- Löschung von Administratoren bei Versetzung oder Beendigung des Arbeitsverhältnisses

4. Kontrolle der Offenlegung

Aspekte der Offenlegung personenbezogener Daten müssen kontrolliert werden: elektronische Übertragung, Datentransport, Übermittlungskontrolle usw. Maßnahmen in Verbindung mit dem Transport, der Übertragung, Kommunikation und Speicherung von Daten auf Datenträgern (manuell oder elektronisch) und für die anschließende Prüfung:

- Verschlüsselung/Tunneling (VPN = Virtual Private Network)
- Elektronische Signatur
- Protokollierung
- Transportsicherheit (SSL)

5. Eingabekontrolle

Datenverwaltung und -pflege müssen vollständig dokumentiert werden. Maßnahmen für die spätere Überprüfung, ob und durch wen Daten eingegeben, geändert oder entfernt (gelöscht) wurden:

- Protokollierungs- und Meldesysteme

6. Jobkontrolle

Die Verarbeitung muss gemäß den Anweisungen durchgeführt werden. Maßnahmen (technisch/organisatorisch) zur Trennung der Verantwortlichkeiten zwischen dem Datenverantwortlichen und dem Datenverarbeiter:

- Eindeutiger Wortlaut des Vertrages
- Formelle Auftragsvergabe (Antragsformular)
- Definitiion von Kriterien für die Auswahl des Datenverarbeiters
- Überwachung der Vertragserfüllung

7. Verfügbarkeitskontrolle

Die Daten müssen gegen zufällige Zerstörung oder Verlust geschützt werden. Maßnahmen zur Gewährleistung der Datensicherheit (physische/logische):

- Sicherungsverfahren
- Spiegelung von Festplatten, z. B. RAID-Technologie
- Unterbrechungsfreie Stromversorgung (USV)
- Remote-Speicherung
- Firewall-Systeme
- Disaster-Recovery-Plan