Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten

1. Zutrittskontrolle

Der unbefugte Zutritt zu den Räumlichkeiten mit den Computern, auf denen personenbezogene Daten gespeichert sind, wird verhindert, indem technische und organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten, getroffen worden sind:

- Zutrittskontrolle durch persönliche Befugnis
- Türsicherung (abgeschlossene Türen)
- Überwachungseinrichtung: Alarmanlage

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme wird verhindert, indem technische (Kennwort-/ Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung getroffen worden sind:

- Passwortvergabe (Benutzername und Passwort)
- Zuordnung von Benutzerprofilen
- Verschlüsselung von Datenträgern

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen werden verhindert, indem das Berechtigungskonzept und die Zugriffsrechte sowie deren Überwachung und Protokollierung bedarfsgerecht ausgestaltet worden sind:

- Differenzierte Berechtigungen der Benutzer (Profile, Rollen, Transaktionen und Objekte)
- Passwortrichtlinie inklusive Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Anzahl der Administratoren auf das „Notwendigste" reduziert

4. Weitergabekontrolle

Bei der Weitergabe personenbezogener Daten (manueller bzw. elektronischer Transport, Übertragung, Übermittlung oder Speicherung auf Datenträger) sowie bei der nachträglichen Überprüfung wurden die folgenden Maßnahmen getroffen:

- Verschlüsselung
- Übermittlungskontrolle
- Protokollierung

5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist gewährleistet. Hierzu wurden Protokollierungssysteme implementiert, mit denen nachträglich überprüft werden kann, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.
Mit Dienstleistern, die Zugriff auf die Daten haben, werden Verträge über die Auftragsverarbeitung personenbezogener Daten geschlossen.

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist gewährleistet. Hierzu wurden technische und organisatorische Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer getroffen. Hierzu zählen:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung

- Kontrolle der Vertragsausführung

7. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust geschützt. Hierzu wurden die folgenden physikalischen und logischen Maßnahmen zur Datensicherung getroffen:

- Backup-Verfahren
- Spiegeln der Daten auf eine zweite Festplatte
- Stromversorgung mit USV
- Umfassender Brandschutz
- Virenschutz/Firewall

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet. Hierzu wurden die folgenden Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken getroffen:

- Berechtigungskonzept
- Logische Mandantentrennung (softwareseitig)
- Versehen der Datenfelder mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Trennung von Geschäftsführungs- und Mitarbeiterdaten