Checkliste

Zur Erfüllung der technischen und organisatorischen Maßnahmen (§10 DSG NRW)

Zutrittskontrolle

Gemeint sind Maßnahmen, die verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden.

- Gebäudesicherung
    - Zäune
    - Pforte
    - Videoüberwachung
- Sicherung der Räume
    - Sicherheitsschlösser
    - Chipkartenleser
    - Codeschlösser
    - Sicherheitsverglasung
    - Alarmanlagen

Zugangskontrolle

Gemeint sind Maßnahmen, die verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können, wobei sich allerdings das Wort "nutzen" nicht auf die Legaldefinition des § 3 Absatz 5 BDSG beschränkt.

- Zugang zu Rechnern/Systemen (Authentifizierung)
    - Benutzerkennung mit Passwort
    - biometrische Benutzeridentifikation
    - Firewall

Zugriffskontrolle

Es muss gewährleistet werden, dass die zur Benutzung von DV-Anlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können für welche sie berechtigt sind **und** das personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

- Berechtigungskonzept
- Benutzerkennung mit Passwort
- gesicherte Schnittstellen (USB, Firewire, Netzwerk, etc.)
- Datenträgerverwaltung

Weitergabekontrolle

Es muss verhindert werden, dass personenbezogenen Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt

gelesen, kopiert, verändert oder gelöscht werden können und das festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist.

- Sicherung bei der elektronischen Übertragung
    - Verschlüsselung
    - VPN
    - Firewall
    - Fax-Protokoll

- Sicherung beim Transport
    - verschlossene Behälter
    - Verschlüsselung

- Sicherung bei der Übermittlung
    - Verfahrensverzeichnis
    - Protokollierungsmaßnahmen

Eingabekontrolle

Es muss sichergestellt werden, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

- Protokollierung
- Benutzeridentifikation

Auftragskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden.

- Weisungsbefugnisse festlegen
- vor-Ort Kontrollen
- Datenschutzvertrag gemäß den Vorgaben nach § 11 DSG NRW
- Stichprobenprüfung
- Kontrollrechte

Verfügbarkeitskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

- Brandschutzmaßnahmen
- Überspannungsschutz
- unterbrechungsfreie Stromversorgung
- Klimaanlage
- RAID (Festplattenspiegelung)
- Backupkonzept
- Virenschutzkonzept
- Schutz vor Diebstahl

Trennungsgebot

Es ist sicherzustellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden getrennt verarbeitet werden können.

- Trennung von Produktiv- und Testsystemen
- getrennte Ordnerstrukturen (Auftragsdatenverarbeitung)
- separate Tabellen innerhalb von Datenbanken
- getrennte Datenbanken

Insbesondere sind allgemein Verschlüsselungsverfahren nach aktuellem Stand der Technik zu berücksichtigen.

Für die Erfüllung der technischen und organisatorischen Maßnahmen gilt ein sog. Verhältnismäßigkeitsprinzip. Demnach müssen personenbezogene Daten nicht unendlich stark geschützt werden, wenn die Maßnahmen dafür wirtschaftlich unangemessen hoch ausfallen würden.

Quelle:
http://www.bfdi.bund.de/bfdi_wiki/index.php/Technische_und_organisatorische_Maßnahmen