**Lernzettel 8: Privatheit**

**1. Definitionen und Konzepte**

* **Privatheit:** Die Kontrolle darüber, wann, wie und in welchem Umfang Informationen über eine Person an andere kommuniziert werden.
* **Datenschutz:** Rechtliche Aspekte des Schutzes personenbezogener Daten.
* **Privatsphäre:** Schutz der physischen Umgebung einer Person.
* **Vertraulichkeit:** Nur autorisierte Personen haben Zugang zu bestimmten Daten.
* **Anonymität/Pseudonymität:** Schutz der Identität, indem Daten nicht zur ursprünglichen Identität zurückverfolgt werden können.

**Lernbrücke:** Privatheit ist ein übergreifender Begriff, der sowohl rechtliche als auch technische Aspekte des Schutzes persönlicher Daten umfasst. Datenschutz und Privatsphäre sind Teilbereiche dieses Konzepts.

**2. Schutzziel: Personenbezogene Daten**

* **Definition nach BDSG:** Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, z.B. Name, Telefonnummer, IP-Adresse.
* **Definition nach DSGVO:** Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, z.B. Name, Kennnummer, Standortdaten, Online-Kennung.

**Lernbrücke:** Die Definition personenbezogener Daten ist entscheidend, da sie festlegt, welche Informationen geschützt werden müssen und wie dieser Schutz zu erfolgen hat.

**3. Schutzmechanismen**

* **Browser Fingerprinting:** Technik zur Identifikation von Nutzern durch einzigartige Merkmale ihres Browsers.
* **Big Data:** Nutzung von Suchanfragen, Sozialnetzen und anderen Datenquellen zur Erstellung von Nutzerprofilen, z.B. für personalisierte Werbung oder Überwachung.
* **Technische Schutzmaßnahmen:**
  + **Kryptographie:** Verschlüsselung von Daten.
  + **Proxies:** Vermittlungsdienste, die die Identität des Nutzers verbergen.
  + **Aggregation und Rauschen:** Techniken zur Datenveränderung, um Anonymität zu bewahren.

**Lernbrücke:** Schutzmechanismen sind notwendig, um die Privatsphäre zu wahren und die Risiken durch die Auswertung großer Datenmengen zu minimieren.

**4. Rechtliche Grundlagen**

* **Deutschland:**
  + **BDSG (Bundesdatenschutzgesetz), TMG (Telemediengesetz), TKG (Telekommunikationsgesetz).**
* **Europa und die Welt:**
  + **DSGVO (Datenschutz-Grundverordnung).**
  + **OECD Guidelines:** Richtlinien zum Schutz der Privatsphäre und des grenzüberschreitenden Flusses personenbezogener Daten.

**Lernbrücke:** Rechtliche Rahmenbedingungen bilden die Basis für den Schutz personenbezogener Daten und regeln die Anforderungen an die Datensicherheit.

**5. Datenschutzprinzipien**

* **Sieben goldene Regeln des Datenschutzes:**
  1. **Rechtmäßigkeit:** Rechtliche Grundlage notwendig.
  2. **Einwilligung:** Datensubjekte informieren und Entscheidungen ermöglichen.
  3. **Zweckbindung:** Daten nur für den Erhebungszweck verwenden.
  4. **Erforderlichkeit:** Nur notwendige Daten sammeln.
  5. **Transparenz:** Informations- und Auskunftsrechte gewähren.
  6. **Datensicherheit:** Schutz durch technische und organisatorische Maßnahmen.
  7. **Kontrolle:** Audits und Datenschutzbeauftragte.

**Lernbrücke:** Diese Prinzipien sind Leitlinien für den verantwortungsvollen Umgang mit personenbezogenen Daten und deren Schutz.

**6. Privacy by Design**

* **Grundprinzipien:**
  1. **Proaktiv, nicht reaktiv:** Vorbeugung statt Schadensbegrenzung.
  2. **Datenschutz als Standardeinstellung.**
  3. **Eingebetteter Datenschutz:** Datenschutz in das Design integriert.
  4. **Volle Funktionalität:** Datenschutz und Sicherheit gleichwertig.
  5. **Durchgängige Sicherheit:** Schutz über den gesamten Lebenszyklus.
  6. **Sichtbarkeit und Transparenz:** Technik sollte prüfbar sein.
  7. **Nutzerzentriert:** Gestaltung benutzerfreundlich und nutzerorientiert.

**Lernbrücke:** Privacy by Design integriert Datenschutz von Anfang an in die Entwicklung von Systemen und Anwendungen, um die Einhaltung von Datenschutzbestimmungen zu gewährleisten.