Informatikklausur - Alles was DU wissen musst!

Thema: Welche moralische und rechtliche Verantwortung tragen Informatiker*innen hinsichtlich des Datenschutzes, Urheberrechts und der gesellschaftl. Auswirkungen informatischer Systeme? Wie kann Datensicherheit (durch Verschlüsselungen) gewährleistet werden?

Datenschutz

Definition: *Schutz des Rechts auf informationelle Selbstbestimmung* (Jeder hat das Recht, selbst über die Preisgabe und Verwendung eigener personenbezogener Daten zu bestimmen. Nicht personenbezogene Daten fallen nicht unter den Datenschutz!)

Grundlagen der DSGVO

Verbot mit Erlaubnisvorbehalt (Erhebung, Speicherung, Weitergabe oder Verwendung personenbezogener Daten ohne Zustimmung der betroffenen Person / ohne gesetzliche Regelung für einen konkreten Zweck ist verboten)
Datenminimierung (So wenig personenbezogene Daten wie möglich sammeln, nach Möglichkeit anonymisieren und löschen sofern nicht mehr benötigt)
Zweckbindung (Erhebung/Verarbeitung personenbezogener Daten nur für einen konkreten Zweck gestattet)
Transparenz (Betroffene Person immer vorab/während Verarbeitung über Verwendung der personenbezogenen Daten vollumfänglich informieren)
Erforderlichkeit (Verarbeitung nur gestattet, sofern die personenbezogenen Daten dafür auch benötigt werden / die Aufgabenerfüllung dadurch erheblich erleichtert wird)
Recht auf Widerruf (Die Einwilligung zur Erhebung/Verwendung/etc. kann jederzeit vom Betroffenen widerrufen werden. Damit ist der weitere Besitz/die weitere Verarbeitung verboten und die Daten müssen gelöscht werden)
Datensicherheit (Definiert durch Sicherheitsziele; Erhobene Daten müssen entsprechend dieser geschützt werden (s.u.))

Urheberrecht

Creative-Commons (CC) -Lizenzsystem als Lösungsversuch, die Rechte anderer über ein eigenes Werk einfach festzulegen. Hinter der Kurzfassung (Commons Deed) steckt dann ein langer, juristischer Volltext und eine maschinenlesbare Fassung

- CC 0
- CC BY
- CC BY NC
- CC BY SA
- CC BY SA NC
- CC BY ND
- *CC BY ND NC (In Klausur nutzbar. Namensnennung, keine Bearbeitung oder kommerzielle Nutzung des Flyers zulässig)*

- -----
- **0** *ist 0* und **verzichtet auf alle urherberrechtlichen Ansprüche**
- **BY** *ist Männchen* und bedetutet **Namensnennung**
- **NC** *ist durchgestr. Euroz.* und bedeutet (non-commercial) **keine kommerzielle Nutzung** ist erlaubt
- **SA** *ist Pfeil entgegen d. Uhrzeigersinns* und bedeutet (share-alike), dass die **Weitergabe unter gleichen Bedingungen** erfolgen muss
- **ND** *ist Gleichzeichen* und bedeutet (no-derivatives) **keine Bearbeitung** erlaubt

<u>Sicherheitsziele</u>
Kommen die dran?
- Vertraulichkeit (Schutz vor Einsicht unberechtigter Personen)
- Integrität (Daten in Originalform, keine Änderung)
- Verfügbarkeit/Zuverlässigkeit (Schutz vor Ausfall von z.B. Server)
- Authentifikation (Identitätsfeststellung vor Datenzugriff)
- Zugriffskontrolle (Nur berechtigte Personen dürfen zugreifen)
- Anonymität (ggf. dürfen Daten nicht einer individuellen Person zugeordnet werden können)
- Unbeobachtbarkeit (Kommunikation unauffällig gestalten bzw. verdecken)
- Verbindlichkeit (Zusagen von Personen dürfen nicht unzulässig abgestritten werden. Lösbar durch z.B. digitale Signatur)

<u>Verschlüsselung</u>
Transposition - Reihenfolge vertauschen, bspw. durch übereinander aufschreiben und dann abwechselnd die Buchstaben nehmen)
Monoalphabetische Substitution (Rotation) - Cäsar-Verschlüsselung mit einem Schlüsselbuchstaben, der die Verschiebung angibt
Polyalphabetische Substitution - Vigenèere-Verschlüsselung, dessen Verschiebung mit einem Schlüsselwort angegeben wird. (Alphabet von 0-25 bei Verschiebung, B wäre also der nächste Buchstabe und nicht der übernächste!!)Chl
Asymmetrische Verschlüsselungsverfahren - AES o.ä. nutzt ein Schlüsselpaar (Schlüssel ist Produkt zweier Primzahlen um einzigartigen Schlüssel zu Gewährleisten) zur Ver- und Entschlüsselung. Jeder kann mit dem Public-Key etwas Verschlüsseln, dies kann jedoch nur wieder mit dem Private-Key entschlüsselt werden.