Repetitionsblatt W1 ManSec: Datenschutz II

1) Erläutern Sie die Begriffe

- **Datenschutz by Design**

> Greift den Grundgedanken auf, dass sich der Datenschutz am besten einhalten lässt, wenn er bereits bei Erarbeitung eines Datenverarbeitungsvorgangs technisch integriert ist.

- **Datenschutz by Default**

> Datenschutzfreundliche Voreinstellungen – Werkeinstellungen sind datenschutzfreundlich auszugestalten. Nach dem Grundgedanken sollen insbesondere die Nutzer geschützt werden, die weniger technikaffin sind und z.B. dadurch nicht geneigt sind, die datenschutzrechtlichen Einstellungen ihren Wünschen entsprechend anzupassen.

2) Beschreiben Sie kurz die Schwierigkeiten das Konzept „Zweckbindung“ in der Praxis einzuhalten.

> Die Zweckbindung definiert die Gründe für die Datenerfassung und Zugriff. Die Verwendung von automatischen Methoden zur Durchsetzung von Datenschutzbestimmungen erfordert, dass der Zweck eines angeforderten Zugriffes automatisch erkannt und gegen die Policy überprüft werden kann.

3) Wie kann verhindert werden, dass die Tester von Applikationen nicht mit den Produktionsdaten arbeiten können und müssen?

> Durch Maskierung von Personendaten wird der Bezug zu den Individuen in der Datenbank zerstört. Es muss aber darauf geachtet werden, dass die Umformung so realistisch und akkurat wie möglich ist; sie muss ebenfalls format- und linksicher sein.

4) Nennen Sie die zwei alternativen Voraussetzungen, damit ihre Firma Personendaten analytisch auswerten kann.

> - Einwilligung (aller im Datensatz involvierten Personen)
> - Anonymisierung der Personendaten

5) Was ist ein Quasi-Identifikator?

> Eine Menge von Attributen (Personendaten), welche zusammen eine Person mit hoher Wahrscheinlichkeit „bestimmbar“ macht.

6) Warum ist k-Anonymität ein Mass, welches die „Qualität“ einer Anonymisierung beschreibt?

> - k Datensätze bilden eine Äquivalenzklasse (bzgl. des Quasi-Identifikators)
> - schützt mit einer Konfidenz von 1/k vor einer ‘korrekten’ Verknüpfung einer Person mit ihren sensitiven Attributen
>
> Damit können die Anonymisierungen verglichen werden: je höher k desto besser!

7) Welche Schritte müssen Sie durchführen, damit Sie eine vorgegebene „k-Anonymität“ erreichen?

> - Bestimmung der Identifikatoren und des Quasi-Identifikators

> - Vorgabe einer Generalisierungsstrategie
> - Entfernen der Identifikatoren
> - Umformen einzelner Attribute aus dem Quasi-Identifikator bis gewünschtes Mass erreicht ist, eventuell unter Zuhilfenahme von Unterdrückung.