

Datenschutzrechtliche Auditierung von Biobanken

Fokus: Datenschutzrecht

Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?

Befund:

Bei Biobanken mit ihren Daten-Probe-Doppelstrukturen funktioniert das Modell des klassischen Datentreuhänders (der auch ein Probentreuhänder sein müsste) nicht.

Reaktion:

Wir brauchen eine betriebliche Alternativlösung für das Fehlen eines vertrauenswürdigen unabhängigen Datentreuhänders bei Biobanken.

Die Herstellung von Vertrauen in die Alternativlösung erfordert dabei

- **Formelle Datentreuhänderschaft** und
- **Materielle Datentreuhänderschaft.**

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Rechtlicher Rahmen – Normative Vorgaben

- Kriterien des Datenschutzrechts
- Kriterien anderer Rechtsmaterien, z.B.
 - Lückenhaftes Humanforschungsrecht außerhalb von AMG-Studien
- Das Fehlen von Regulierung, z.B.
 - fehlendes Forschungsgeheimnis, vgl. NER 2003, These 20

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Umsetzung der normativen Vorgaben

Was muss die Biobank für ein Audit tun?

- Identifikation der tatsächlichen Anknüpfungspunkte für datenschutzrechtliche Kriterien
- Beschreibung der tatsächlichen Anknüpfungspunkte für Kriterien
 - Beschreibungsweise ist durch den Zweck bestimmt =
Durch Standardisierung:
 - Vertrauen stiften
 - Kosten senken

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Umsetzung der normativen Vorgaben:

Was muss die Biobank für ein Audit tun?

- Beschreibung des allgemeinen Biobank-Geschäftsmodells
- Beschreibung der Aufbau- und Ablauforganisation insbesondere derjenigen wesentlichen Elemente, die mit Aussicht auf Standardisierung beschreibbar sind
 - Identifikation der Kriterien (Normen), die dafür gelten
 - Beschreibung der zugeordneten Anknüpfungspunkte

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Weiterer Gang der Darstellung:

1. Übersichten

1. Allgemeine Geschäftsmodellbeschreibung

1. Rechtliche Kriterien der Geschäftsmodellbeschreibung
2. -> Gegenstände und Anknüpfungspunkte der Geschäftsprozessmodellbeschreibung

2. Aufbau- und Ablauforganisation

1. Rechtliche Kriterien der Aufbau- und Ablauforganisation
2. -> Gegenstände und Anknüpfungspunkte der Beschreibung der Aufbau und Ablauforganisation

2. Detaildarstellung (Beispiel)



***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Allgemeine Geschäftsmodellbeschreibung

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Rechtliche Kriterien der Geschäftsmodellbeschreibung

- Kriterien des Datenschutzrechts, z.B.:
 - Datensparsamkeit, §§ 4a BDSG, 4 LDSG-SH
 - Voraussetzung: spezifiziertes Geschäftsmodell
 - Datensicherheit, §§ 9 BDSG, 5 LDSG-SH, DatenschutzVO
 - Voraussetzung: spezifiziertes Geschäftsmodell
 - Datenschutzbeauftragter § 4f Abs. 1 BDSG
 - Verfahrensverzeichnis §§ 4g Abs. 2, 4e Satz 1 Nr. 1 – 8 BDSG
 - Überprüfte Verhaltensregeln § 38a BDSG

Welche Datenschutzkriterien gelten für Biobanken? Wie muss man die Kriterienerfüllung erkennbar machen?

Rechtliche Kriterien der Geschäftsmodellbeschreibung

1981 – Regulierungsempfehlung des Europarats

R1981 (1) vom 23.1.1981

Regulierungsempfehlung zu den Rechtsverhältnissen bei automatisierten medizinischen Datenbanken - Nrn. 2.2 und 3

- Öffentliche Pflichtmitteilung -> Tatsache der Betriebsaufnahme
- Verpflichtender Inhalt der Mitteilung:
 - Name der medizinischen Datenbank
 - Zusammenfassung des betrieblichen Regelwerks
 - Hinweis auf das Verfahren einer detaillierten Unterrichtung über das betriebliche Regelwerk
- Index zum Mindestinhalt des betrieblichen Regelwerks

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Rechtliche Kriterien der Geschäftsmodellbeschreibung

2006 – Regulierungsempfehlung des Europarats

R 2006 (4) vom 15.3.2006

Regulierungsempfehlung für Biobanken

Article 19

1. Each population biobank should be subject to independent oversight, in particular to safeguard the interests and rights of the persons concerned in the context of the activities of the biobank.
2. **Regular audits should be conducted** of the implementation of procedures on access to, and use of, samples.

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Gegenstände und Anknüpfungspunkte der Geschäftsmodellbeschreibung

Selbstbeschreibung:

1. Polycys zu Akquisition, Weitergabe und nachgeholter Transparenz
2. Polycys zu Verfahren bei der Ausübung von Spenderrechten
3. Internes Regelwerk zu Handhabungsabläufen (SOPs)
4. Standardschriftwerk zu externer Verwendung
5. Dokumentation von Verwendungsbedingungen
(Optionsausübungen zum Standardschriftwerk)
6. Allgemeine Risikobeschreibung, Datenschutzkonzept
- 7. Beschreibung der Aufbauorganisation**
- 8. Beschreibung der Ablauforganisation**



***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Aufbauorganisation +
Ablauforganisation

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Kriterien des Datenschutzrechts zur Aufbau- und Ablauforganisation:

1. Grundsätzliche technische Ausgestaltung
 1. Datensparsamkeit, Anonymisierung, Pseudonymisierung (Methoden und Implementation)
 2. Transparenz und Aktualität der Verfahrensbeschreibung
2. Zulässigkeit der Datenverarbeitung
 1. Rechtsgrundlagen für Erheben, Verarbeiten, Übermitteln (Anforderungen an die Einwilligung und ihre Implementation)
 2. Allgemeine Grundsätze und Pflichten

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Kriterien des Datenschutzrechts zur Aufbau- und Ablauforganisation:

1. Technisch-organisatorische Begleitmaßnahmen
2. Datenschutzrechte des Spenders
3. Datenschutzkonformität der Protokollierungsvorgänge

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Aufbau- und Ablauforganisation
Gegenstände und Anknüpfungspunkte der Selbstbeschreibung

1. Prozesse
2. Rollen, Inkompatibilitäten von Rollen
3. Verbindung von Prozessen mit Rollen
4. Kommunikationen (authentisch, integer, vertraulich)
5. Systeme und Subsysteme (Probenlager, Datenbanksystem, ...)
6. Protokollierung der Daten- und Probenverwendung
7. Schutzgegenstände (Identifikation z.B. durch Datenfeldbeschreibung)
8. Keine Einbruchstellen für Umgehungslösungen

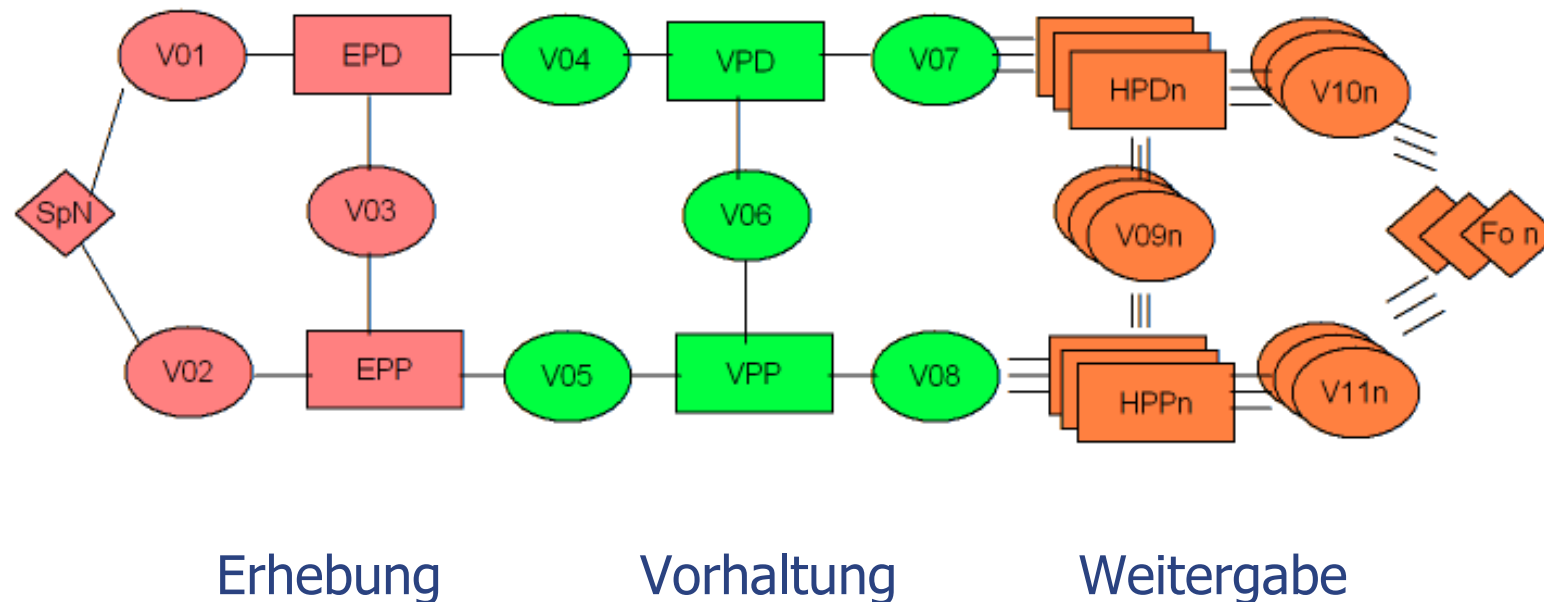
***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Detaildarstellung (Beispiel):

Gestreckte Pseudonymisierung in Biobanken

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

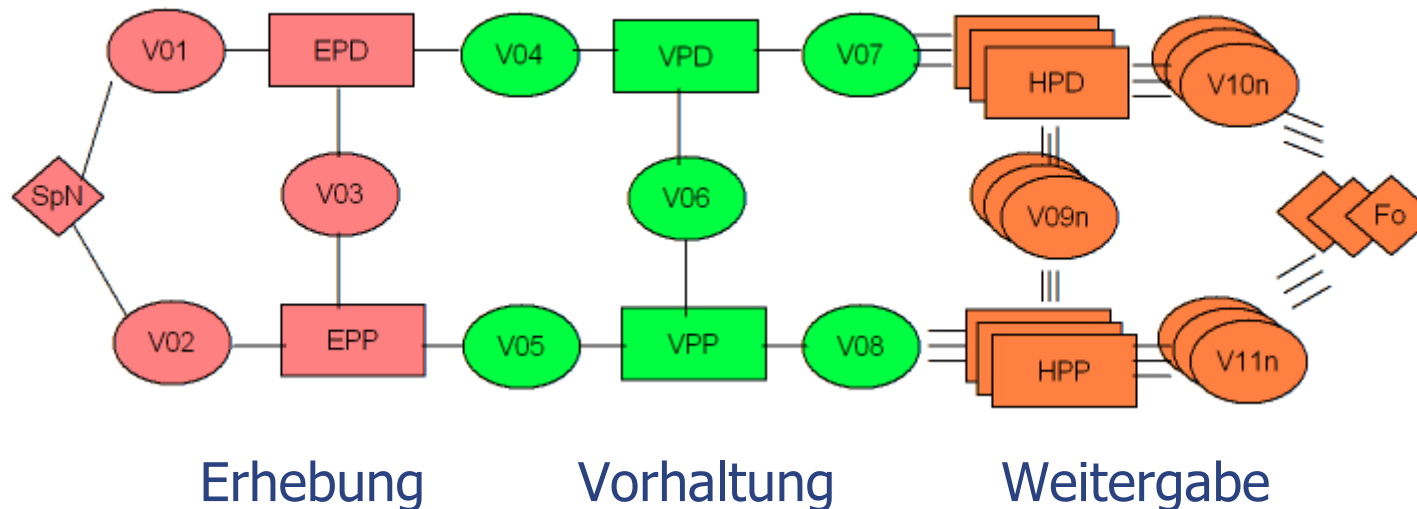
**Pseudonymisierung in Biobanken als gestreckter Vorgang
mit drei Risikosphären unterschiedlicher Beherrschbarkeit**



Welche Datenschutzkriterien gelten für Biobanken? Wie muss man die Kriterienerfüllung erkennbar machen?

Die Risikosphären des Modells verstehen

- Nicht jedes Pseudonym muss in jeder Biobank vorkommen
- Abhängig von ...:
 - „Wo beginnt und endet die Biobank als organisatorisch-rechtliche Einheit?“
 - Welche Risikoschwellen gibt es?



***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Normvorgabe Pseudonymisierung:

Nur die Namen von den medizinischen Daten abtrennen,
ein Pseudonym vergeben
- und schon tritt die Pseudonymisierung ein?

§ 3 Absatz 6a BDSG - Pseudonymisierung

Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

-> „Pseudonymisierung“=

Pseudonymvergabe + datensparsame Behandlung der Studiendaten

Was heißt das für die Biobank?

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Gestreckte Pseudonymisierung /Übersicht

Die Daten werden schrittweise verändert ...:

- Erhebung,
- Erster Pseudonymtausch, Erhalt der Probe-Daten-Verkettung
- Datensparsame Eingangsbehandlung
- Vorhaltung für wechselnde Studien
- Zusammenstellung zur Beforschung an eine einzelne Studie
- Erneute datensparsame Behandlung (nun studienbezogen)
- Zweiter Pseudonymtausch, Erhalt der Probe-Daten-Verkettung

-> Pseudonymisierung als gestreckter Prozess mit 3 Risikosphären

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Gestreckte Pseudonymisierung /Genauer betrachtet

Warum kommt es bei der Biobank für die Phase der Vorhaltung zu unvollständiger Pseudonymisierung?

1. Organisatorische Streckung: die Streckung durch die Teilprozesse der Erhebung, Vorhaltung und Herausgabe:

- Pseudonymisierung kann nicht vor Weitergabe zur Beforschung an eine einzelne Studie abgeschlossen sein.
- Ihr Zuschnitt kann von Studie zu Studie wechseln.
- Vor dieser Weitergabe zur Beforschung ist Pseudonymisierung notwendigerweise unvollständig.
- Genau dies macht das **Geschäftsmodell der Biobank** mit seinem studienübergreifend vorgehaltenen Daten- und Probenbestand aus.

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Gestreckte Pseudonymisierung /Genauer betrachtet

Warum kommt es bei der Biobank für die Phase der Vorhaltung zu unvollständiger Pseudonymisierung?

2. Methodenbedingte Streckung:

Unverfälschten Beforschbarkeit erfordert: Spenderdaten können nur nach **einheitlich wirkender Regel** in den Zustand versetzt werden, den sie für wechselnde Zwecke der Beforschung haben müssen. Individualisierende Daten-Ausreißer können nicht „für den Datenschutz weggehobelt“ werden.

3. Zeitliche Streckung bei künftiger Zunahme technischer Möglichkeiten der Probenanalytik oder der Datenauswertung (z.B.: Eintritt einer identifizierenden Wirkung von Biomarkermustern).

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

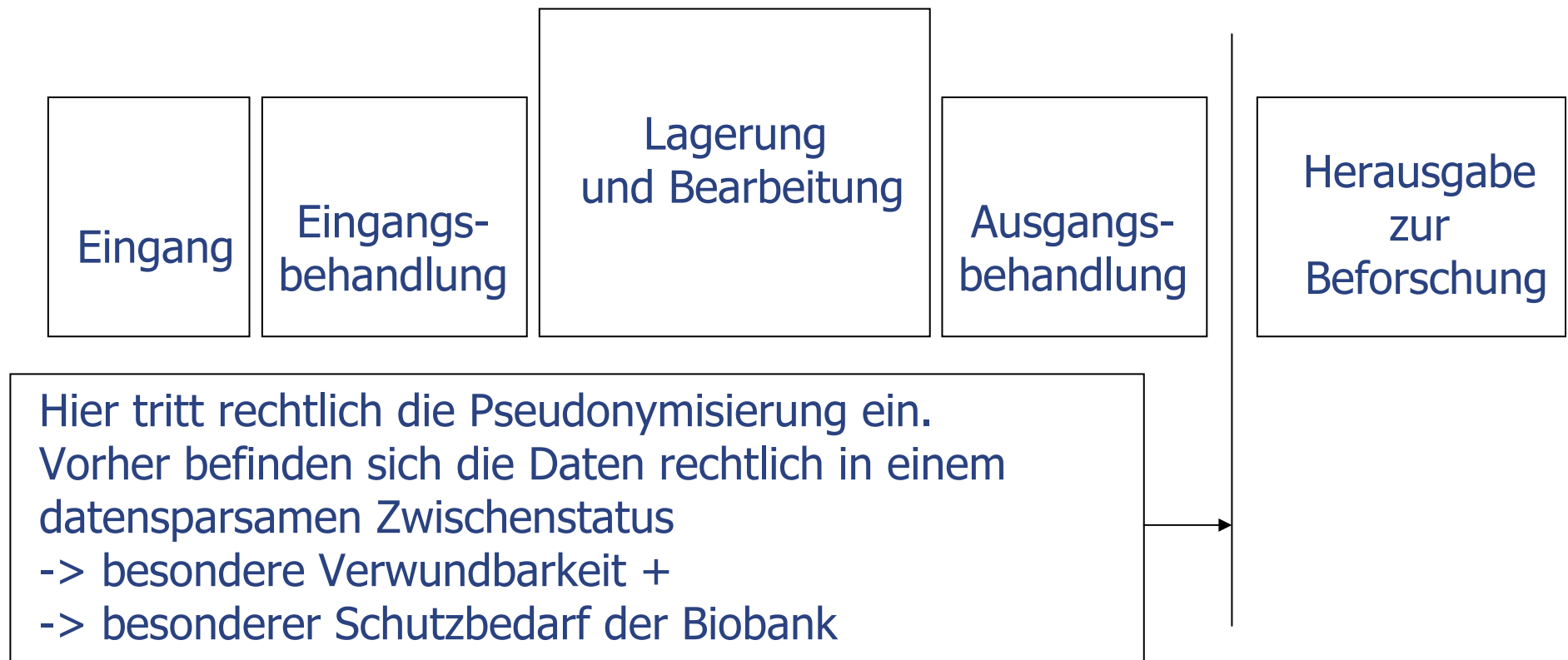
Gestreckte Pseudonymisierung /Genauer betrachtet

Warum kommt es bei der Biobank für die Phase der Vorhaltung zu unvollständiger Pseudonymisierung?

4. unvollständige Pseudonymisierung durch **zeitliche Streckung** bei spenderbezogenem **Datenrücktransfer der Forschung an die Biobank**
5. unvollständige Pseudonymisierung durch das **Dispositionsinteresse der Biobank an der Erhaltung ihrer Wahlmöglichkeit**, zwischen anonymisierter oder pseudonymisierter Herausgabe an die Forschung
6. unvollständige Pseudonymisierung durch das **Dispositionsinteresse der Biobank an breiter Beforschbarkeit**
7. Für Daten Ausgeführtes gilt entsprechend für Proben.

Datenschutzrechtliche Auditierung von Biobanken Spenderschutz durch Datentreuhänderschaft

Gestreckte Pseudonymisierung /Ergebnis:



***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Gestreckte Pseudonymisierung:

Anforderungen an die Selbstbeschreibung,
insbesondere zu Prozessen und Rollen

Welche Datenschutzkriterien gelten für Biobanken? Wie muss man die Kriterienerfüllung erkennbar machen?

Anknüpfungspunkte für Kriterien zur Pseudonymisierung Umsetzung der Pseudonymisierung in betriebliche Rollen und Prozesse

1. Trennung von Daten:

- Wer trennt wann wo nach welchen Methoden?
- Welche Systeme datenschutzfördernder Technik werden benutzt?
- Was tun diese Systeme?

2. Zuweisung getrennter Daten an getrennte Aufgaben

- Definition einer abschließenden Aufgabenliste

3. Definition von Rollen

- Definition eines abschließenden Rollenkonzepts
 - Insbes.: Wer ist für Systeme datenschutzfördernder Technik verantwortlich?
- Definition inkompatibler Rollen,
- Inkompatibilität und Stellvertretung
- Zuordnung der Prozesse zu den Rollen

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

**Anknüpfungspunkte für Kriterien zur Pseudonymisierung
Umsetzung der Pseudonymisierung in betriebliche Rollen und Prozesse**

- 4. Umsetzung der Pseudonymisierung in betriebliche Rollen und Prozesse**
- 5. Zuweisung getrennter Aufgaben an getrennte Rollen**
 1. Darlegung eines konsistenten und vollständigen Zuweisungskonzepts
 2. Ausweisung getrennter Rollen und ihrer Weisungsverhältnisse
- 6. Zuweisung besonderer Rollen an besondere (rechtlich verselbständigte) Stellen**

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

**Anknüpfungspunkte für Kriterien zur Pseudonymisierung
Weitere Umsetzungsmaßnahmen**

1. Definition von Prozessverbindungen (**Kommunikationen** in der gestreckten Pseudonymisierung)
2. Definition von **Kommunikationsmodalitäten**
(Anforderungen der Kommunikationen an Authentizität, Integrität, Vertraulichkeit)
3. Definition von **Systemen** (z.B. Probenlager, Datenbanksystem)
4. Definition der **Protokollierung** der Daten- u. Probenverwendung
5. Definition der **Schutzgegenstände** nach Identifikation und wechselbezoglicher Zuordnung

***Welche Datenschutzkriterien gelten für Biobanken?
Wie muss man die Kriterienerfüllung erkennbar machen?***

Besten Dank!

Wolfgang Zimmermann
zimmermann@datenschutzzentrum.de