Ein Weg zu datenschutzgerechten Sicherheitstechnologien

Walter Peissl
Maren Raguse

Gliederung

- Das PRISE Projekt: Ziele, Struktur und Definitionen
- Sicherheitstechnologien und Einsatz-Szenarien
- Auf dem Weg zu datenschutzkonformen Sicherheitstechnologien
  - Bestehende ISO Standards in anderen Bereichen
  - Folgen für die Sicherheitsforschung
  - Kriterien für datenschutz-konforme Sicherheitstechnologien

PRISE – die Ziele

- *Entwicklung von Kriterien und Richtlinien zur grundrechtskonformen Sicherheitsforschung und Technikentwicklung*
- Wissensbasis
  - Technologien
  - Rechtsrahmen
- Einsatz-Szenarien
- Partizipative Technikfolgenabschätzungs-Verfahren in 6 europäischen Staaten
- Weiterentwicklung der Kriterien und Richtlinien unter Einbeziehung von
  - Anbietern von Sicherheitstechnik,
  - privaten und öffentlichen Anwendern,
  - Gestaltern der Sicherheitspolitik und von
  - Organisationen, die zur Sicherheitspolitik möglicherweise in Konflikt stehende Interessen vertreten
- Verbreitung der Ergebnisse

PRISE Partner

Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften
Wien, AT

Teknologirådet,
København, DK

Unabhängiges Landeszentrum für Datenschutz, Kiel, DE

Teknologirådet,
Oslo, NO

Sicherheit und Privatsphäre

- Gesellschaftliche Sicherheit
- Bedrohung durch Personen und Gruppen von Personen
- Sicherheitstechnologien und Sicherheitsmaßnahmen
- Beinträchtigung der Privatsphäre

Sicherheits-Basistechnologien

- Telekommunikationstechnologien
- Sensortechnologien
- Biometrie
- Datenspeicherung, -analyse und Entscheidungsunterstützung

Telekommunikationstechnologien

- Festnetztelefonie
- Mobiltelefonie
- Kommunikation über das IP
- Lokalisierungsdienste
- Satelliten gestützte Ortungssysteme

- Abhören und Überwachen der Kommunikation
- Telefon, Internet, Briefe
- Grundsätzlich Eingriff in die Privatsphäre
- Ortung (zeitlich und räumlich)

Sensortechnologien

- Durchleuchtungssysteme
- Elektro-optische Sensoren (CCTV)
- Akustische Sensoren
- Unbemannte Luftfahrzeuge
- RFID
- Maschinenlesbare Reisedokumente
- Identitätskarten

- Metalldetektoren
- „Nackte Maschine“
- Aktive und passive Kameras
- Automatische Gesichtserkennung
- Kennzeichen von Autos
- Verdächtiges Verhalten
- Fälschliche Verdächtigung
- Aufbewahrungszeit der Daten

Biometrie

- Grundsätzliches zum Prozess
- Fingerabdrücke
- Gesichtserkennung
- Iriserkennung
- DNA-Profil
- Ethische Fragen zur Biometrie

- „Körperliche“ Merkmale
- Fingerabdruck, Gesicht, Iris, Stimme ...
- Authentifizierung, Identifikation
- Identitätsdiebstahl
- „Falsch positiv“ und „falsch negativ“

Datenspeicherung, -analyse und Entscheidungsunterstützung

- Datenbanken
- Data Mining
- Suchtechnologien

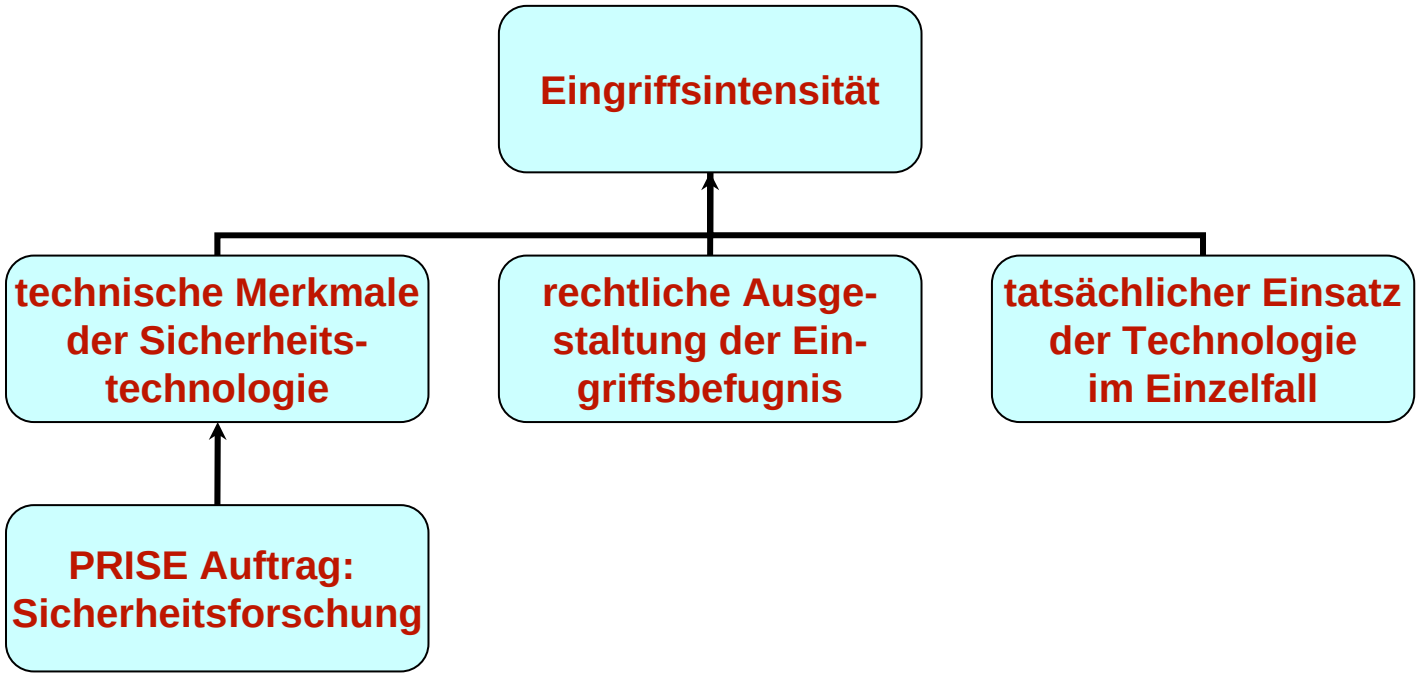
- Tendenz zu mehr Daten
- Längere Speicherung
- Zweckentfremdung
- Verknüpfung unterschiedlicher Datenbanken

Interview Meeting

- Beteiligungsform (pTA) mit quantitativen und qualitativen Aspekten
- In 6 Ländern (D, DK, N, A, H, E)
- ca. 30 Laien je Land/Event
- Bewertung der Szenarien via Fragebogen
- Diskussion der Thematik in Kleingruppen

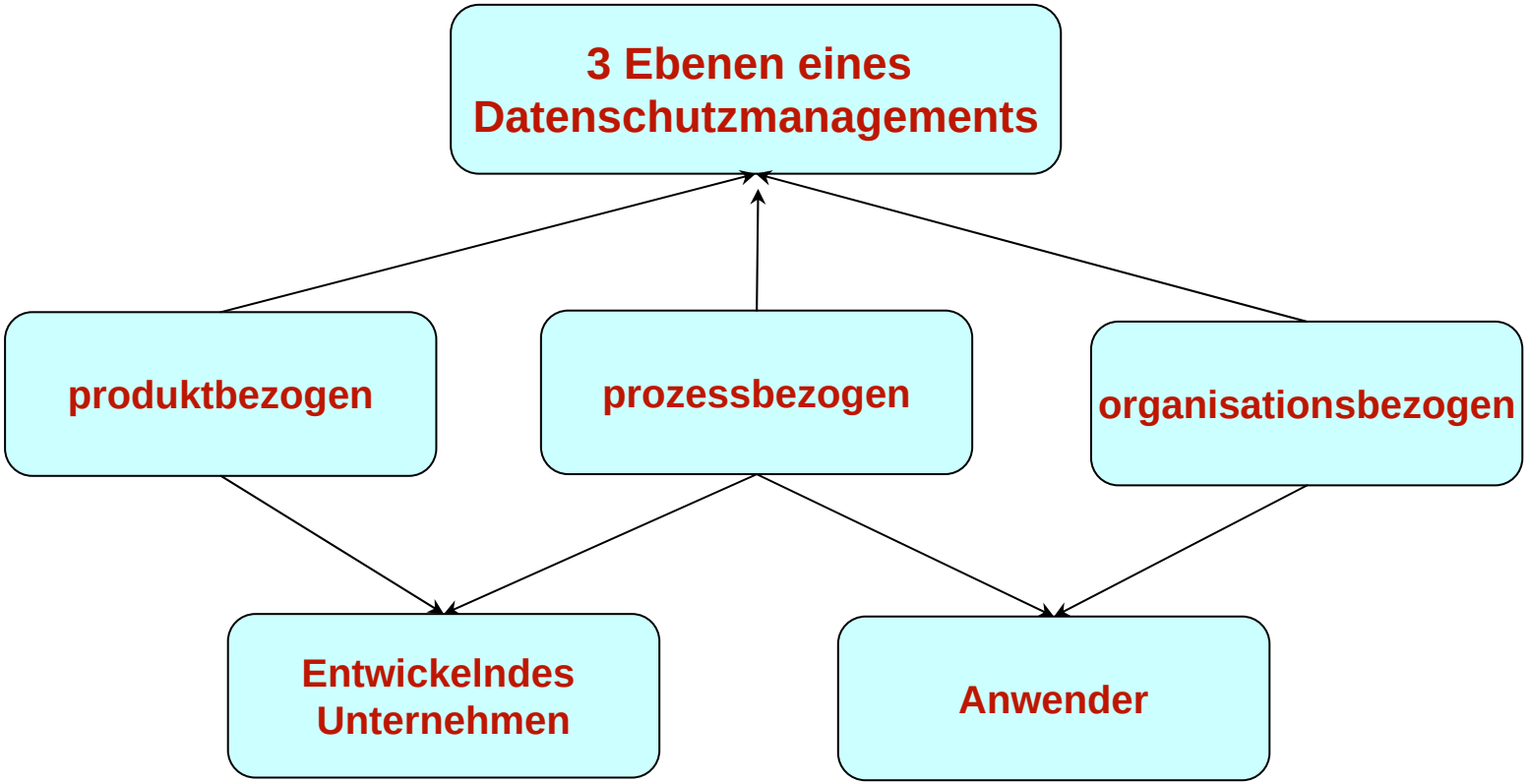
Drei Faktoren der Eingriffsintensität

Beim Einsatz von Sicherheitstechnologien (ob durch öffentliche oder private Stellen) können drei Faktoren die Eingriffsintensität der Maßnahme beeinflussen:



Drei Ebenen des Datenschutzmanagements

Um datenschutzkonforme Sicherheitstechnologien zu realisieren, reicht es nicht, Kriterien nur für das Produkt zu entwickeln, sondern schon bei der Gestaltung des Entwicklungsprozesses ist das Ziel der Datenschutzkonformität zu beachten



Maßstab für Konformität: OECD Richtlinie und EU-Datenschutzrichtlinie

- Rechtmäßigkeit
- Zweckbindung
- Verhältnismäßigkeit
- Transparenz
- Qualität der Daten
- Datensicherheit

Einschränkung der Datenschutzprinzipien im Rahmen polizeilicher Ermittlungsbefugnisse?

- Das Grundrecht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet; BVerfGE 65, 1
- Art. 13 EU-Datenschutzrichtlinie: die Mitgliedsstaaten können einschränken, *sofern eine solche Beschränkung notwendig ist für*

  a) die Sicherheit des Staates, […]
  c) die öffentliche Sicherheit,
  d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten […]

Eingeschränkte Geltung der Datenschutzprinzipien auch für Sicherheitstechnologien?

→ **nein**

- Art. 13 bezieht sich auf R*echtsvorschriften*
- Technologiegestaltung begrenzt Eingriffsintensität
- Datenschutzkonformität der Technologie ermöglicht tatsächlich das mildeste Mittel

Warum betrachten wir IT-Sicherheitsstandards?

- anwendbar auf Organisationen (Unternehmen und Behörden)
- es gibt produktbezogene, prozessbezogene und organisationsbezogene Standards
- IT: Vertraulichkeit, Integrität und Verfügbarkeit
- DS: Datensicherheit und Qualität der Daten

➔ aufgrund dieser Überschneidung von Datenschutz und IT-Sicherheit wurde im Rahmen des BSI-Grundschutzes kürzlich ein Datenschutzbaustein veröffentlicht

Bestehende Standards IT-Sicherheit

produktbezogen

Common Criteria
(ISO 15408)

prozessbezogen

Grundschutz
(ISO 27001)

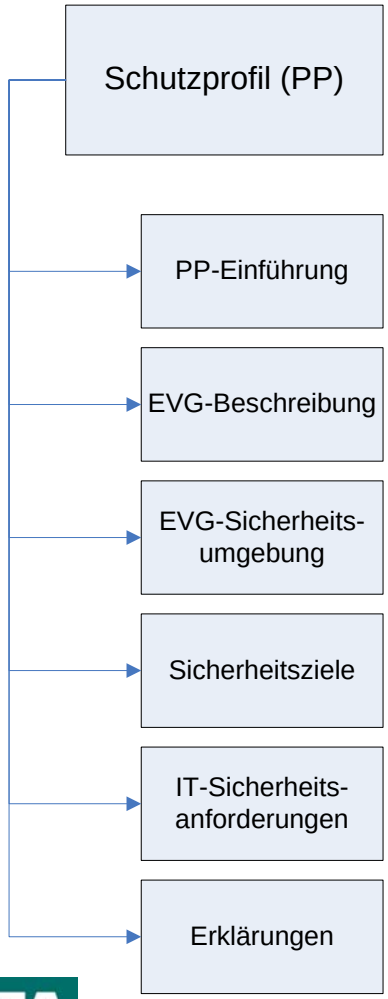
organisationsbezogen

Grundschutz
(ISO 27001)

Managementsystem für
IT-Sicherheit (ISMS)

Unterstützend: Risikoanalyse mit
ISO 17799/27002

Bestehende Standards IT-Sicherheit : produktbezogen



- Common Criteria: Kriterien für Prüfung und Bewertung der Sicherheit von Informations*technik*

Vorgehensweise: Schutzprofile als verallgemeinerte Sicherheitsvorgaben für Evaluationsgegenstand (EVG); Anforderung an Funktionalität und Vertrauenswürdigkeit decken Sicherheitsziele ab; Erklärungsteil erleichtert Umsetzung

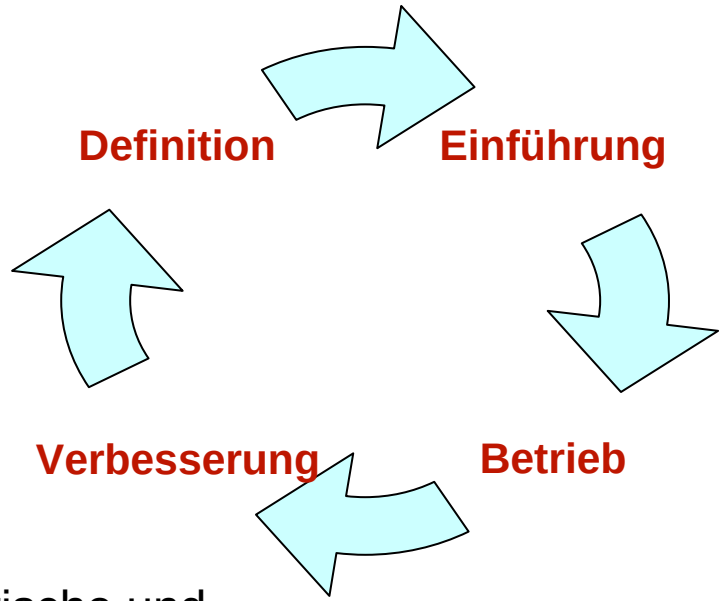
Beispiel: BSI-PP-0023-2007: Schutzprofil Software zur Verarbeitung von personenbezogenen Bilddaten

Bestehende Standards IT-Sicherheit : prozess- und organisationsbezogen

Ziel: Konformität mit Anforderungen aus Gesetzen, Normen, Regeln (z.B. Betriebsvereinbarungen oder Verträgen mit Dritten)

Anwendungsobjekt: IT-Verbund

Phasen: Definition, Einführung, Betrieb, Verbesserung eines InformationsSicherheits-ManagementSystems



Mittel: Risikoanalyse

Grundschutz beinhaltet organisatorische und technische Maßnamen zur Erreichung des Sicherheitsniveaus

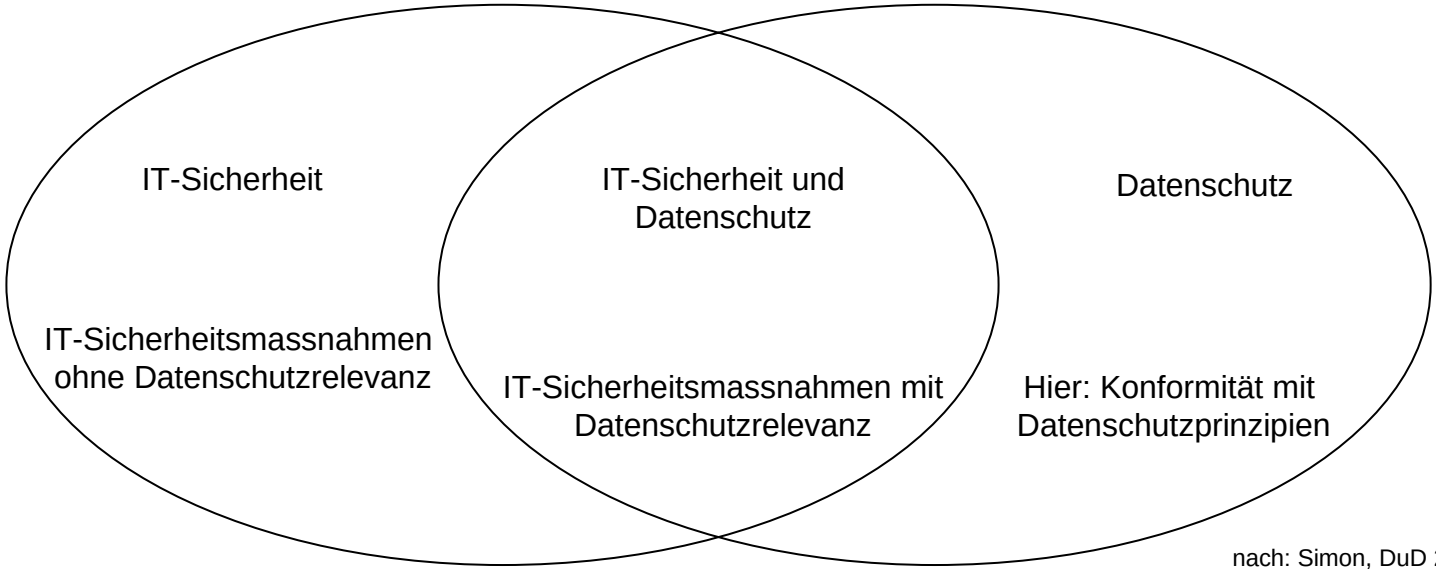
Vorgehensweise nach Grundschutz

1. IT-Strukturanalyse
2. Schutzbedarfsfeststellung:
   - drei Schutzbedarfskategorien: „normal“, „hoch“, „sehr hoch“
   - Definition anhand von möglichen Schäden
   - Für jede IT-Anwendung und jedes IT-System ist der Schutzbedarf hinsichtlich

     Vertraulichkeit Integrität Verfügbarkeit

     zu dokumentieren
3. IT-Grundschutzanalyse:
   - Modellierung: welche Bausteine mit welchen Maßnahmen sind auf welche Räume, Systeme, Anwendungen anzuwenden?
4. Realisierungsplanung für Umsetzung defizitärer Maßnahmen

Folgen für die Sicherheitsforschung



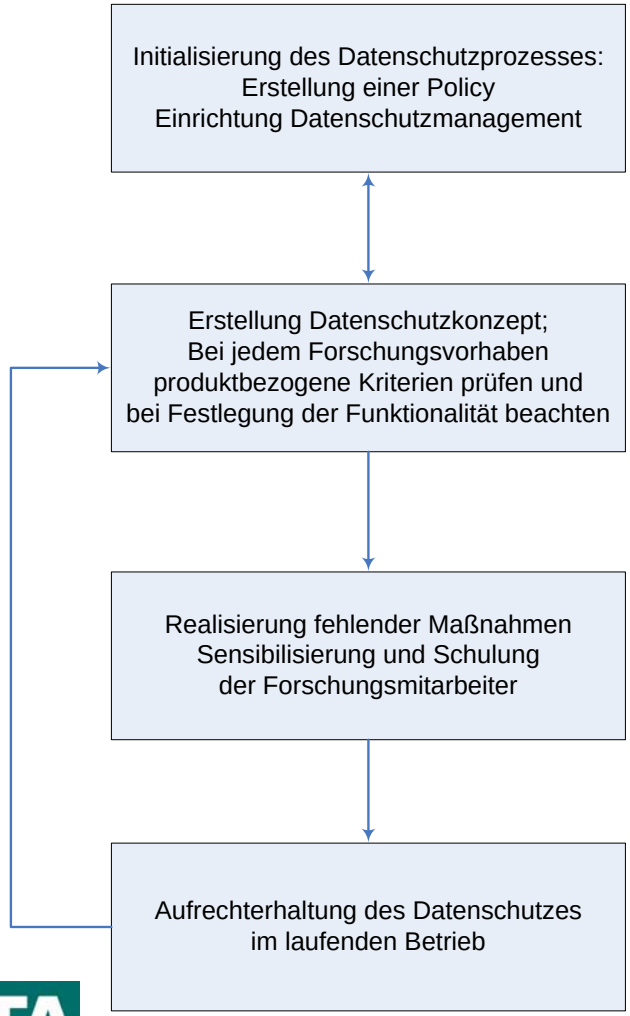
nach: Simon, DuD 2/2007

- bestehende IT-Sicherheitsstandards zielen auf Vertraulichkeit, Integrität und Verfügbarkeit: Datensicherheit und Qualität der Daten als Prinzipien abgedeckt
- Ziel des Datenschutzmanagement in der Sicherheitsforschung: Compliance mit übrigen Datenschutzprinzipien

PRISE Ansatz

Ebene	Anwendungs-objekt	Adressat
Prozessbezogen	F&E Prozess	F&E
Produktbezogen	Sicherheitstechnik	F&E
Prozessbezogen	Polizeiliche Datenverarbeitung	Anwender (Polizei)
Organisationsbezogen	Polizeibehörde	Anwender (Polizei)

Datenschutzmanagement im F&E Prozess

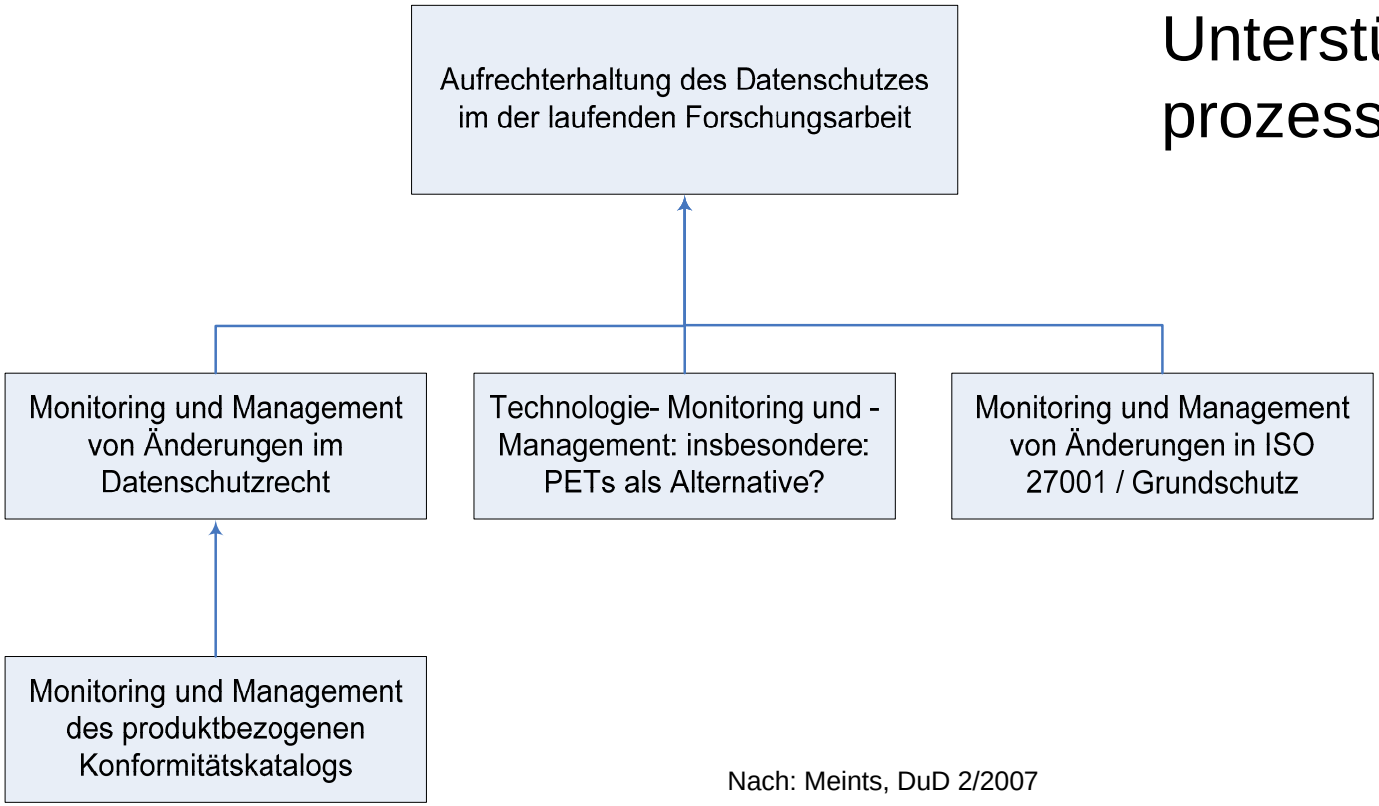


Ziel:
in den Forschungsunternehmen über Managementmaßnahmen die Einhaltung von Datenschutzvorgaben in der Forschungsarbeit sicherzustellen

Nach: Meints, DuD 2/2007

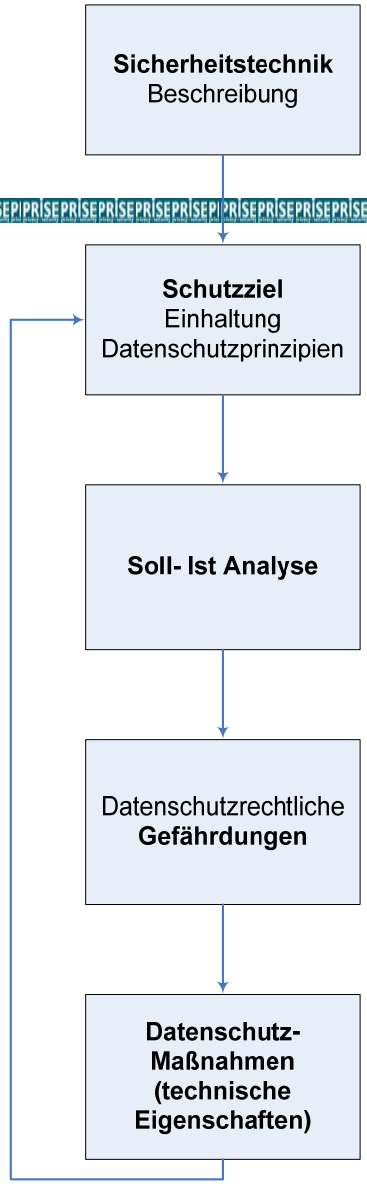
Datenschutzmanagement im F&E Prozess

Unterstützungs-prozess DSM



Nach: Meints, DuD 2/2007

Sicherheitstechnik



generisches Modell einer produktbezogenen Betrachtung

Nach: CC, Datenschutzbaustein Grundschutz

Vielen Dank für Ihre Aufmerksamkeit!

Walter Peissl
wpeissl@oeaw.ac.at.ac.at
http://www.oeaw.ac.at/ita/
+43 1 51581 6584

Maren Raguse
LD104@datenschutzzentrum.de
http://www.datenschutzzentrum.de
+ 49 431 988 1284