Datenschutzrechtliche Rahmenbedingungen für das SELMA-Projekt

Hintergrund Datenschutzrecht (1)

- Einführung
  - Hintergrund: Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983
  - „Recht auf informationelle Selbstbestimmung“; Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG
    - „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“
    - unabhängig davon, ob Daten die Intimsphäre oder Privatsphäre des Einzelnen betreffen „unter den Bedingungen der modernen Datenverarbeitung gibt es keine belanglosen Daten mehr“
  - Verbot mit Erlaubnisvorbehalt
    - Eingriff in Recht auf informationelle Selbstbestimmung nur mit Einwilligung des Betroffenen oder auf gesetzlicher Grundlage

Hintergrund Datenschutzrecht (2)

- Anforderungen des BVerfG an den Gesetzgeber bzgl. datenschutzrechtlicher Normen
  - Bereichsspezifische Datenschutzregelungen
  - Einwilligung des Betroffenen (falls keine gesetzliche Grundlage)
  - Gebot der Direkterhebung
  - Unabhängige Kontrollinstanzen
  - Technisch-organisatorische Schutzvorkehrungen
  - Prozessuale Rechte des Betroffenen
  - Grundsatz der Datensparsamkeit / der Datenvermeidung
  - Zweckbindungsgebot
  - Normenklarheit
  - Verhältnismäßigkeitsgrundsatz

Die Systematik der Gesetzgebung

Datenschutzrechtliche Normen

Allgemeine Datenschutzgesetze

- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetze (LDSG)

Bereichspezifische Datenschutzgesetze

- Telekommunikationsdatenschutz-verordnung (TDSV)
- Teledienstedatenschutzgesetz (TDDSG)
- Signaturgesetz (SigG)

Anwendungsvorrang

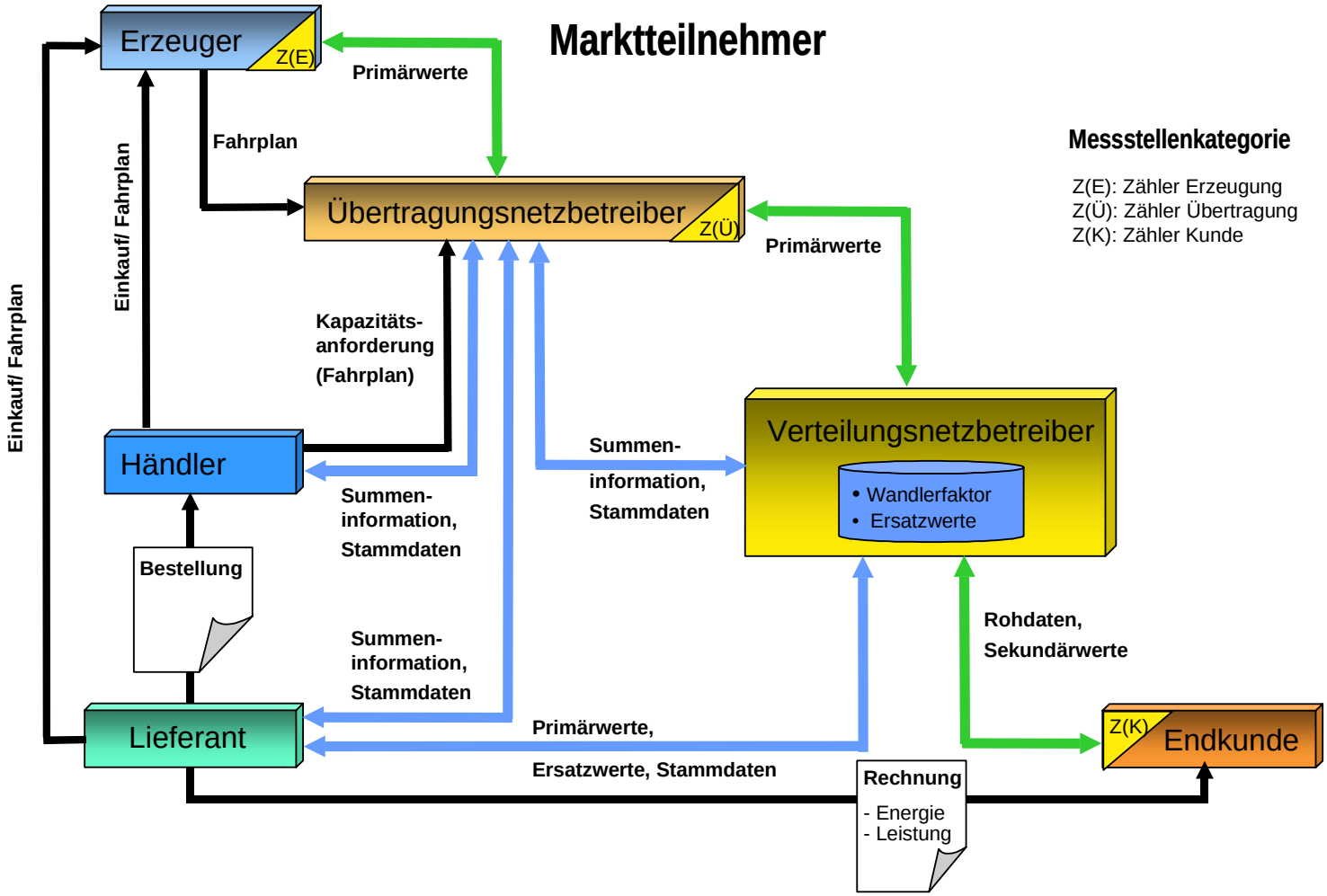
- Bereichsspezifisches vor allgemeinem Datenschutzrecht
- Bundesrecht vor Landesrecht

- Datenschutzrechtliche Anforderungen an das SELMA-Projekt

  (orientiert am Modul „Datenschutz“ im IT-Grundschutzhandbuch des BSI)

  - Sachverhaltsklärung
  - Personenbezug der bei SELMA anfallenden Daten
  - einschlägige Rechtsvorschriften
  - zu ergreifende Maßnahmen

Sachverhaltsklärung



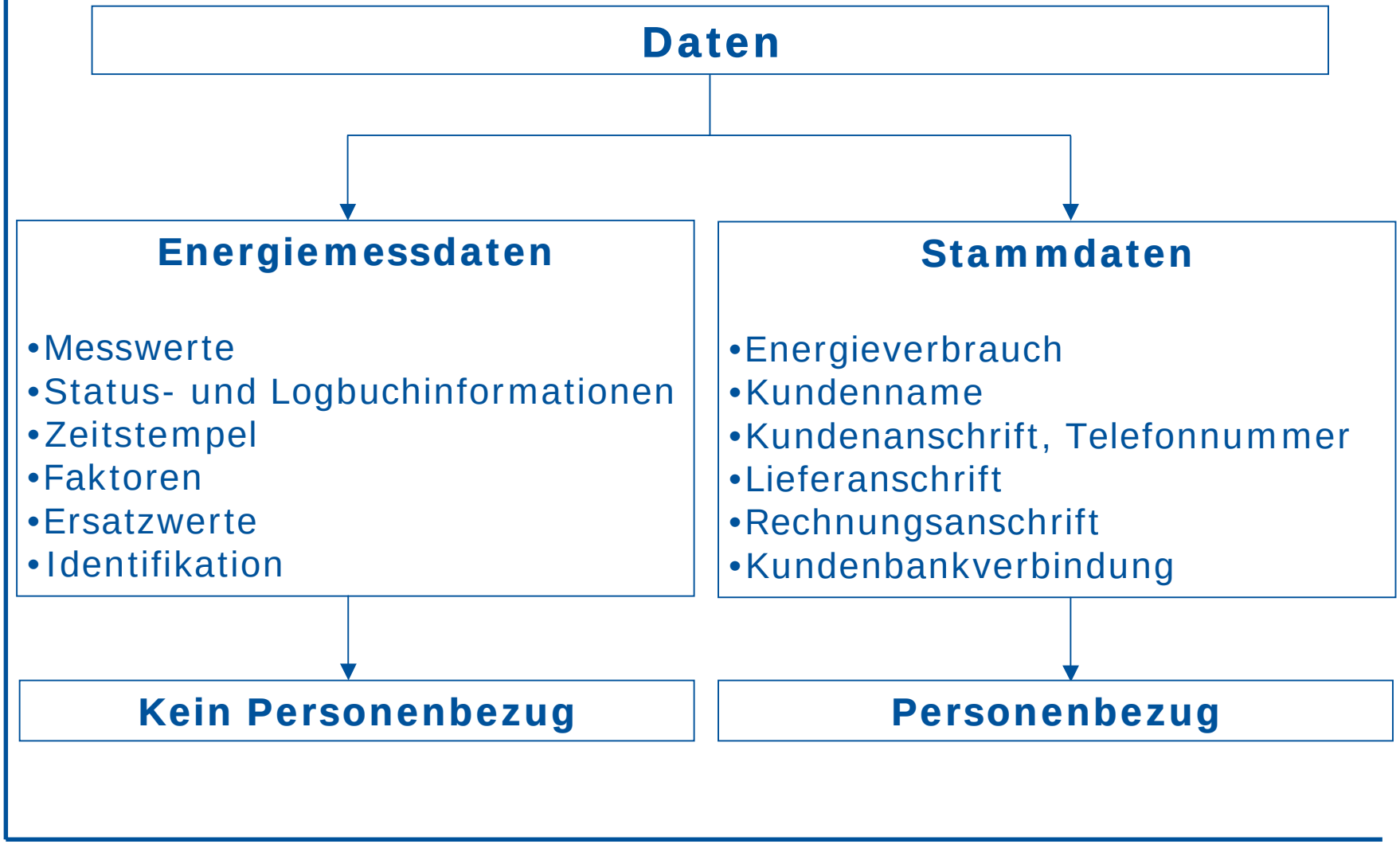
Personenbezug der anfallenden Daten (1)

- Definition „personenbezogene Daten“ (§ 3 Abs. 1 BDSG): „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“
- Problem: Bestimmbarkeit der Person
  - ist gegeben, „wenn zwar nicht durch die Daten alleine, aber durch weiteres legal zugängliches Zusatzwissen – ggf. mit Unterstützung mathematisch-statistischer Verfahren und externer Datenverarbeitungskapazität – die Person von der datenverarbeitenden Stelle identifiziert werden kann“
  - entfällt, wenn die Zuordnung einen unverhältnismäßigen großen Aufwand an Zeit, Kosten und Arbeitskraft erfordert

Personenbezug der anfallenden Daten (2)

- Personenbezug entfällt
  - bei pseudonymisierten Daten:
    liegen dann vor, wenn Name einer Person oder anderes Identifikationsmerkmal durch ein Kennzeichen zu dem Zweck ersetzt wird, um die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren
  - bei aggregierten Daten (von mindestens drei natürlichen Personen)
  - bei juristischen Personen (z.B. GmbH und AG) oder Personenmehrheiten wie Personengesellschaften (z.B. GbR oder OHG) = Sondervertragskunden

Personenbezug der anfallenden Daten (3)



Anwendbare Gesetze

- Telekommunikationsgesetz i.V.m. Telekommunikations-Datenschutzverordnung
  - betrifft unternehmensinterne Telekommunikation; Datenschutzkonformität durch SELMA-Projektpartner vorausgesetzt
- Teledienstedatenschutzgesetz
  - betrifft Bestands- und Nutzungsdaten beim geplanten Abruf der Verbrauchsdaten im Internet
  - sonst Ausnahmevorschrift des § 1 Abs. 1 Nr. 2 TDDSG für Steuerung von Arbeits- und Geschäftsprozessen innerhalb von Unternehmen
- Signaturgesetz
  - (-), da keine personenbezogenen Daten anfallen, da Messwerte pseudonymisiert (der Messstelle zugeordnet)
- Landesdatenschutzgesetze
  - (-), gelten nur für öffentliche Stellen (z.B. Landesbehörden)
- Bundesdatenschutzgesetz als Auffangvorschrift anwendbar

Zu ergreifende Maßnahmen (1)

- Gewährleistung einer zulässigen Datenverarbeitung
  - Einwilligungsklausel in Netznutzungs- und Netzanschlussverträgen
    - schriftlich, textlich hervorzuheben, Belehrungspflicht (§ 4a BDSG)
  - Rechtsgrundlage in § 28 Abs. 1 Satz 1 Nr. 1 BDSG – Verarbeitung personenbezogener Daten zur Erfüllung des Vertragszwecks zulässig
  - §§ 5, 6 Abs. 1 TDDSG für Verarbeitung von Bestands- und Nutzungsdaten beim Bereitstellen der Messdaten im Internet

Zu ergreifende Maßnahmen (2)

- Einhaltung des Grundsatzes der Datenvermeidung / des Erforderlichkeitsgrundsatzes
  - durch Pseudonymisierung
  - möglichst späte Verknüpfung von personenbezogenen Stammdaten und anonymisierten Messwerten (entsprechend § 30 Abs. 1 Satz 2 BDSG)
  - gemäß §§ 5, 6 Abs. 1 TDDSG für Bestands- und Nutzungsdaten bei der Bereitstellung der Energiedaten für den Endkunden im Internet

Maßnahmen:

- Getrennte Speicherung von Energiedaten und personenbezogenen Stammdaten (unter Berücksichtigung der Verhältnismäßigkeit)
- Zugriffsbefugnisse entsprechend Aufgabenzuweisung

Zu ergreifende Maßnahmen (3)

- Einhaltung des Zweckbindungsgrundsatzes
  - Daten dürfen nur zu dem Zweck verarbeitet werden, zu dem sie erhoben worden sind

Maßnahmen:

- Beschränkung und Überprüfung der Möglichkeit zur Auswertung bzw. Verknüpfung der Stammdaten
- Vergabe von Zugriffsrechten, Protokollierungspflichten

Zu ergreifende Maßnahmen (4)

- Beachtung des Datengeheimnisses
  - Sicherung der Vertraulichkeit personenbezogener Daten

Maßnahmen:

- Löschung nicht benötigter Daten
- Einsatz von Verschlüsselungsverfahren (insb. bei Übertragung über offene Netze; im Rahmen der Verhältnismäßigkeit)
- Verpflichtung der Mitarbeiter
- System der Zugriffsbefugnisse

Zu ergreifende Maßnahmen (5)

- Gewährleistung der technischen und organisatorischen Sicherheit der Datenverarbeitung
  - gemäß Anlage zu § 9 BDSG

Maßnahmen:

- Zutrittskontrolle – Zutritt zur Datenverarbeitungsanlage
- Zugangskontrolle – Nutzung von Datenverarbeitungsanlagen
- Zugriffskontrolle – durch Vergabe von Zugriffsberechtigungen
- Weitergabekontrolle – geschützte Weitergabe von Daten
- Eingabekontrolle – Nachvollziehbarkeit der Eingabe von Daten
- Auftragskontrolle – Verarbeitung nach Weisung des Auftraggebers
- Verfügbarkeitskontrolle – Schutz gegen Verlust
- Trennungsgebot – zu unterschiedlichen Zwecken erhobene Daten sind getrennt zu verarbeiten

Zu ergreifende Maßnahmen (6)

- Wahrung der Rechte des Betroffenen
  - Auskunftsrechte (§ 34 Abs. 1 BDSG)
  - Recht auf Berichtigung, Sperrung, Löschung (§ 35 BDSG)

Maßnahmen:

- Gestaltung der Datenverarbeitungssysteme mit dem Ziel, dass Rechte auf Auskunft, Berichtigung, Sperrung und Löschung durchgesetzt werden können

- Einhaltung des Transparenzgrundsatzes
  - Pflichten zur Dokumentation (Angaben aus § 4e BDSG)
  - Meldepflichten gegenüber den Aufsichtsbehörden (§§ 4d, 4e BDSG)

Zu ergreifende Maßnahmen (7)

- Gewährleistung der Datenschutzkontrolle
  - Interne IT-Revision und Datenschutzkontrolle
    - Kontrolle der Verfahren auf Einhaltung der Rechtsgrundlagen und Zweckbestimmung
    - Sicherstellung der Rechte der Betroffenen
    - Unterrichtung über und Verpflichtung der Mitarbeiter auf den Datenschutz
    - Kontrolle der technisch-organisatorischen Maßnahmen
    - Kontrolle der Umsetzung des IT-Sicherheitskonzepts
  - in der Phase der Entwicklung und Erprobung durch das SELMA-Konsortium
  - beim späteren Einsatz durch betriebliche Datenschutzbeauftragte

- Zusammenfassung und Ausblick
  - Datenschutzrechtliche Anforderungen an SELMA-Projektpartner
  - dienen dem Schutz auf informationelle Selbstbestimmung
  - schaffen Akzeptanz beim Kunden
  - tragen zum Erfolg von SELMA bei