PD Dr. Ariane Berger

4. Kommunaler IT-Sicherheitskongress 2017

„Umsetzung der Leitlinie für Informationssicherheit des IT-Planungsrats in Kommunalverwaltungen“

DEUTSCHER LANDKREISTAG

Datenschutzgrundverordnung, NIS-Richtlinie und andere aktuelle Entwicklungen

PD Dr. Ariane Berger

DEUTSCHER LANDKREISTAG

A. Einleitung
B. Datenschutz
   I. DatenschutzgrundVO
   II. Nationale Begleitgesetzgebung
   III. Kommunalrelevanz
   IV. Weitere Entwicklungen auf europäischer Ebene
C. IT-Sicherheit
   I. NIS-Richtlinie
   II. Umsetzungsstand Deutschland
   III. Kommunalrelevanz
D. Fazit

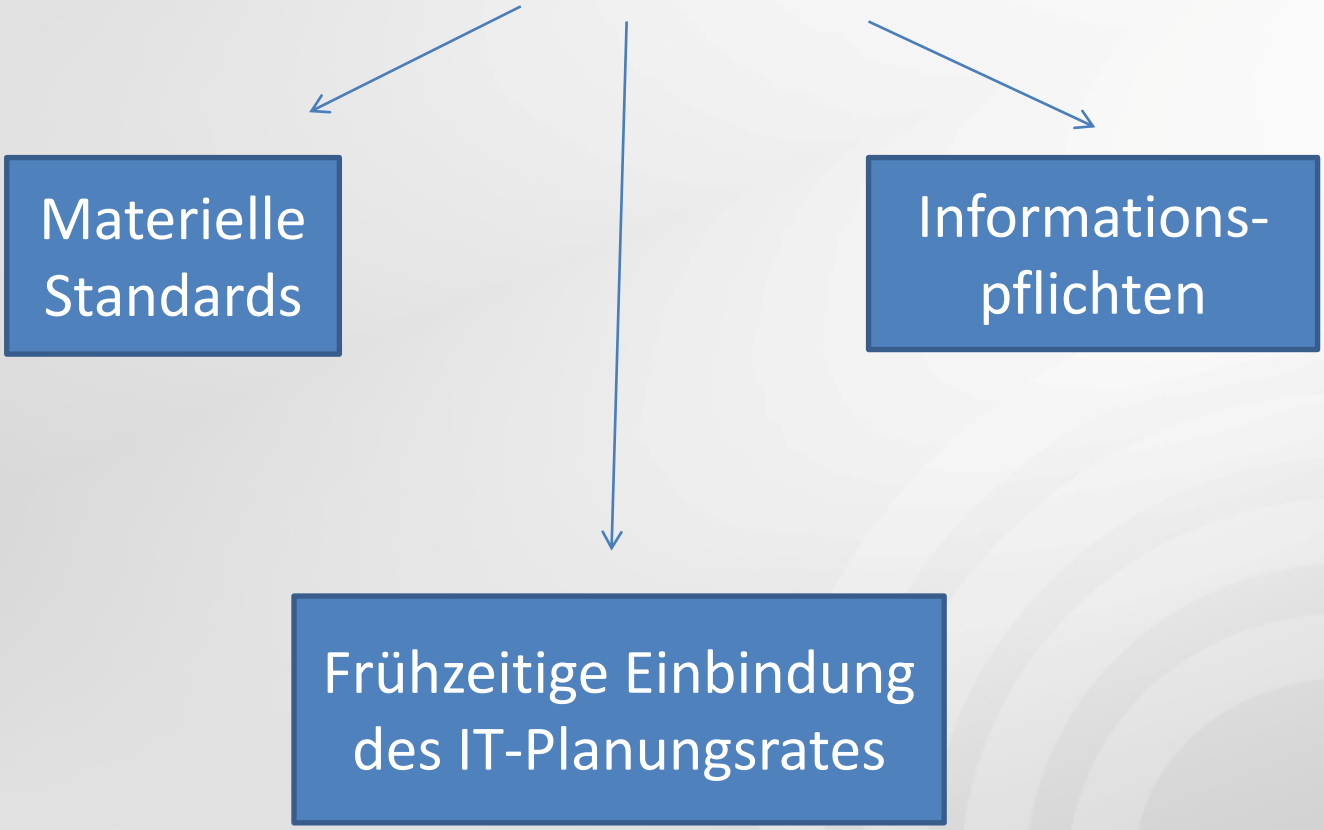
DEUTSCHER LANDKREISTAG

A. Einleitung: Verfassungsrechtliche Ausgangslage

- Gewährleistung von Datenschutz und IT-Sicherheit:
  - Staatliche Infrastrukturverantwortung
  - Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
- Gesetzgebungs- und Verwaltungskompetenzen der Länder zwingen Bund zu „kooperativem Föderalismus“
- Grundrechte und EU-Grundfreiheiten der Wirtschaftsteilnehmer zwingen ebenfalls zu kooperativem Ansatz

DEUTSCHER LANDKREISTAG

Allgemeine Regelungsstrategie des Bundes



DEUTSCHER LANDKREISTAG

B. Datenschutz

I. DatenschutzgrundVO

II. Nationale Begleitgesetzgebung

III. Kommunalrelevanz

IV. Weitere Entwicklungen auf europäischer Ebene

DEUTSCHER LANDKREISTAG

I. DatenschutzgrundVO

- Sog. personenbezogene Daten werden aktuell durch die **EU-Datenschutzrichtlinie** geschützt
- Diese wird im **Mai 2018** durch die **EU-Datenschutzgrundverordnung** abgelöst
- Wesentliche Inhalte:
  - Grundsätze der Transparenz, Zweckbindung und Datenminimierung
  - Pflichten für Datenverarbeiter
  - Korrespondierende Rechte der Betroffenen
  - Mindeststandards für die Verarbeitung personenbezogener Daten
  - Schadensersatzansprüche und Bußgeldtatbestände
  - Zusammenarbeit der nationalen Aufsichtsbehörden bei grenzüberschreitender Datenverarbeitung

DEUTSCHER LANDKREISTAG

II. Nationale Begleitgesetzgebung

- Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die unionsrechtlichen Datenschutzvorgaben (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – **DSAnpUG-EU**) im Gesetzgebungsverfahren:
  - Bundesdatenschutzgesetz (**BDSG**) wird grundlegend reformiert
  - Bereichsspezifische Änderungen u.a. des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes und des Sicherheitsüberprüfungsgesetzes
- Achtung: **Ab Mai 2018** „überwölbt“ die **DatenschutzgrundVO** die nationale Rechtsordnung (Bundes- und Landesdatenschutzgesetze, Verwaltungsverfahrensgesetze u.a.) und geht diesen im Kollisionsfall vor.

DEUTSCHER LANDKREISTAG

Aufbau des BSDG-E

- Teil 1 des BDSG-E enthält allgemeine Bestimmungen:
  - Schaffung allgemeiner Rechtsgrundlagen für die Datenverarbeitung durch öffentliche Stellen und die Videoüberwachung
  - Regelungen zu Datenschutzbeauftragten öffentlicher Stellen
  - Ausgestaltung der unabhängigen Datenschutzaufsichtsbehörden
  - Festlegung der deutschen Vertretung im Europäischen Datenschutzausschuss
  - Rechtsbehelfe

- Teile 2 bis 4 des BDSG-E enthalten bereichsspezifische Regelungen

DEUTSCHER LANDKREISTAG

§ 3 BDSG-E

Verarbeitung personenbezogener Daten durch öffentliche Stellen

Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

DEUTSCHER LANDKREISTAG

Grundprinzipien des personenbezogenen Datenschutzes nach DatenschutzgrundVO

- Rechtmäßigkeit, Treu und Glauben und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Begrenzung der Speicherdauer
- Integrität und Vertraulichkeit
- Rechenschaftspflicht des Verantwortlichen

DEUTSCHER LANDKREISTAG

III. Kommunalrelevanz

- Adressaten des **BDSG-E**:
  - Öffentliche Stellen des Bundes
  - Öffentliche Stellen der Länder einschließlich der Kommunen, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen
  - Nichtöffentliche Stellen
- Adressaten der **DatenschutzgrundVO**:

  Jede Stelle, die personenbezogene Daten automatisiert verarbeitet, auch Kommunen
- **IT-Planungsrat** koordiniert Ausarbeitung gemeinsamer unions- und bundesrechtskonformer Datenschutzstandards für Landes- und Kommunalverwaltungen

DEUTSCHER LANDKREISTAG

IV. Weitere Entwicklungen auf europäischer Ebene

- EU-Kommission plant einheitlichen Regelungsrahmen für die „Europäische Datenwirtschaft“
- Soll personenbezogene und nicht-personenbezogene Daten erfassen
- 1.1.2017: Kommission hat einen **„Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation“** vorgelegt
- Weitere Reformvorschläge folgen

DEUTSCHER LANDKREISTAG

Wesentliche Regelungsinhalte des EU-Reformpaketes:

- Regulierung von internetbasierten Kommunikationsdiensten wie Web.de, Whatsapp oder Skype
- Schaffung von Zugangsregelungen
- Festlegung allgemeiner Datenschutzstandards
- Haftungsregelungen für Gerätehersteller, Datenproduzenten und Datennutzer
- Definition der „Dateneigentümerschaft“
- Lokalisierungsbestimmungen, d.h. Vorschriften zum Speicherort
- Drittstaatenregelungen

DEUTSCHER LANDKREISTAG

C. IT-Sicherheit

I. NIS-Richtlinie

II. Umsetzungsstand Deutschland

III. Kommunalrelevanz

DEUTSCHER LANDKREISTAG

- RL 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (**NIS-Richtlinie**)
- **bis Mai 2018** in nationales Recht umzusetzen
- **Zielsetzung** der NIS-Richtlinie:
  - EU-weiter Aufbau nationaler Kapazitäten für die Cyber-Sicherheit
  - Stärkere Zusammenarbeit der Mitgliedsstaaten der Europäischen Union
  - Festlegung von Mindestsicherheitsanforderungen
  - Festlegung von Meldepflichten

DEUTSCHER LANDKREISTAG

II. Umsetzungsstand Deutschland

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-Sicherheitsgesetz**) in Kraft (**Artikelgesetz**)
- Ausführungsverordnung **BSI KritisVO** (Teil 1 in Kraft, Teil 2 im Rechtssetzungsverfahren)
- Noch im Gesetzgebungsverfahren:
  - Änderungen im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (**BSIG**)
  - Branchenspezifische Anpassungen u.a. im Atomgesetz (**AtG**), Energiewirtschaftsgesetz (**EnWG**) und Sozialgesetzbuch V (**SGB V**)
- Durchführungsrechtsakte der EU-Kommission, die das erforderliche Sicherheitsniveau und Meldeschwellen festlegen, stehen noch aus

DEUTSCHER LANDKREISTAG

Wesentliche Regelungsinhalte des IT-Sicherheitsgesetzes:

- Vorgaben für IT-Sicherheitsstandards und Meldepflichten für IT-Sicherheitsvorfälle
- Zielgruppe:
  - Bundesverwaltung
  - Betreiber Kritischer Infrastrukturen (sog. KRITIS-Betreiber)
  - Definiert in der BSI KritisVO
- Regelschwellenwert: 500.000 versorgte Personen
- Aufgabenzuwachs beim BSI:
  - Nationale IT- und Cybersicherheitsbehörde
  - BSI zentrale Anlaufstelle für KRITIS-Betreiber
  - Einrichtung von Mobile Incident Response Teams (MIRTs)
  - Informations- und Veröffentlichungspflichten

DEUTSCHER LANDKREISTAG

III. Kommunalrelevanz

- Adressaten des IT-Sicherheitsgesetzes gemäß § 2 Abs. 10 BSIG i.V.m. BSI KritisVO:
  - Kritische Infrastrukturen
  - Bundesverwaltung
- Kommunale Verwaltungen als kritische Infrastrukturen?
- Kommunalwirtschaftliche Unternehmen als kritische Infrastrukturen?

DEUTSCHER LANDKREISTAG

Koordinierungsaufgabe des IT-Planungsrates:

- Einführung eines einheitlichen Informationssicherheits-Managements in Anlehnung an BSI-Grundschutz, unabhängig von „Kritikalität“
- Umsetzung einheitlicher Mindeststandards in der Informationssicherheit
- Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung
- Gemeinsame Abwehr von Angriffen auf IT-Systeme der Verwaltung
- Sensibilisierungsmaßnahmen zur Informationssicherheit

DEUTSCHER LANDKREISTAG

D. Fazit

- Die Kommunen müssen sich jetzt mit den neuen Datenschutz- und IT-Sicherheitsaufgaben befassen
- Der IT-Planungsrat koordiniert eine bundeseinheitliche Festlegung von Datenschutz- und IT-Sicherheitsstandards

DEUTSCHER LANDKREISTAG

Vielen Dank für Ihre Aufmerksamkeit!