Datenschutz im JI-Bereich: Was gilt für Owi-Verfahren und Gefahrenabwehr?

Sommerakademie 2019

Infobörse 10

Barbara Körffer

Unabhängiges Landeszentrum für Datenschutz

Übersicht

- **Überblick über Vorschriften**

  Welche Vorschriften gelten für JI-Bereich und DSGVO-Bereich?

- **Anwendungsbereiche**

  Wann und für wen gilt was?

- **Inhalte der Regelungen**

  Welche wesentlichen Unterschiede gibt es zwischen JI-Bereich und DSGVO?

ÜBERBLICK ÜBER ANWENDBARE VORSCHRIFTEN

DSGVO für öffentliche Stellen

- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung): unmittelbar anwendbares Recht

- Ergänzend dazu, sofern die DSGVO nationale Regelungen zulässt:
  - Bereichsspezifische Regelungen
  - LDSG 1. und 2. Abschnitt

„JI-Richtlinie“

- Richtlinie (EU) 2016/680 („JI-Richtlinie“) gilt nicht unmittelbar, sondern muss durch die Mitgliedstaaten durch eigene Vorschriften umgesetzt werden
- „JI“: Justiz und Inneres
- **Umsetzungsvorschriften im deutschen Recht**
  - LDSG 3. Abschnitt: allgemeine Regelungen
  - Bereichsspezifische Regelungen, z.B.
    - Landesverwaltungsgesetz
    - Justizvollzugsdatenschutzgesetz
    - Maßregelvollzugsgesetz
    - Strafprozessordnung
    - BKA-Gesetz

ANWENDUNGSBEREICHE DSGVO UND „JI-RICHTLINIE“

Gesetzliche Regelung – Anwendungsbereich 3. Abschnitt LDSG

§ 20 LDSG – Anwendungsbereich

Die Vorschriften dieses Abschnitts gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Dies schließt den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten zuständigen öffentlichen Stellen mit ein. Die öffentlichen Stellen gelten dabei als Verantwortliche. Die Sätze 1 bis 3 finden zudem Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung von Strafen, von Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs, von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und von Geldbußen zuständig sind. Soweit dieser Teil Vorschriften für Auftragsverarbeiter enthält, gilt er auch für diese.

Anwendbarkeit JI-Regelungen für folgende Zwecke

Strafverfolgung und Verfolgung von Ordnungswidrigkeiten

- JI-Regelungen anwendbar für alle Stellen, die für diese Aufgaben zuständig sind, soweit sie Daten für diese Zwecke verarbeiten.

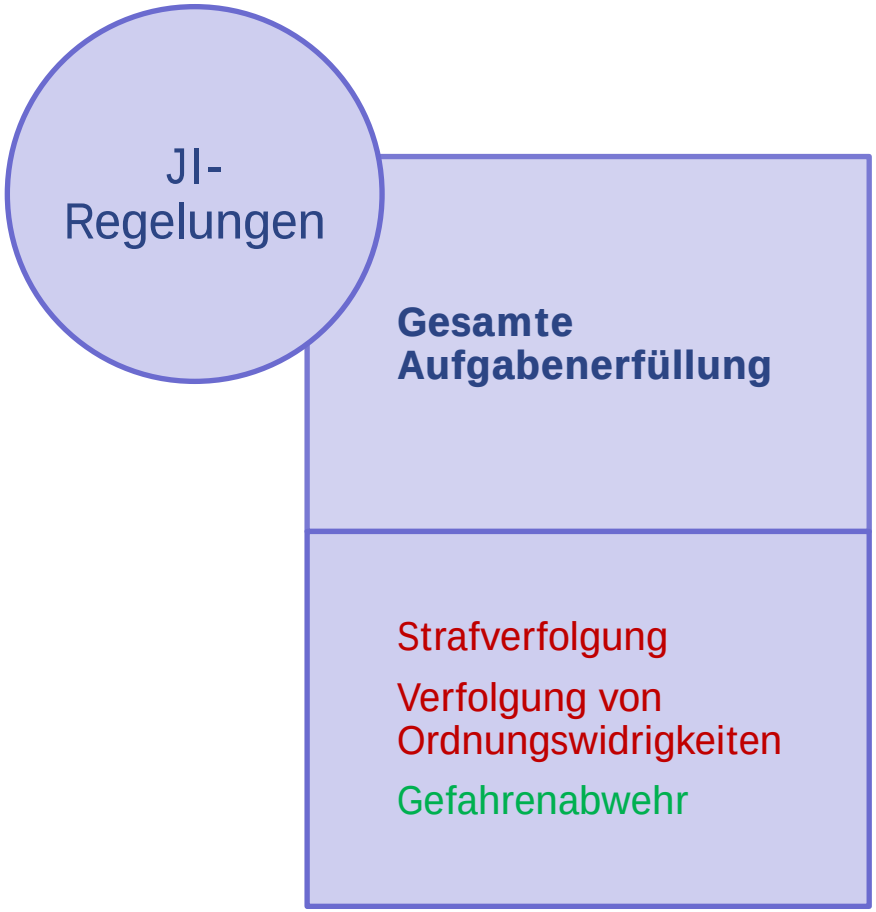
Abwehr von Gefahren für die öffentliche Sicherheit

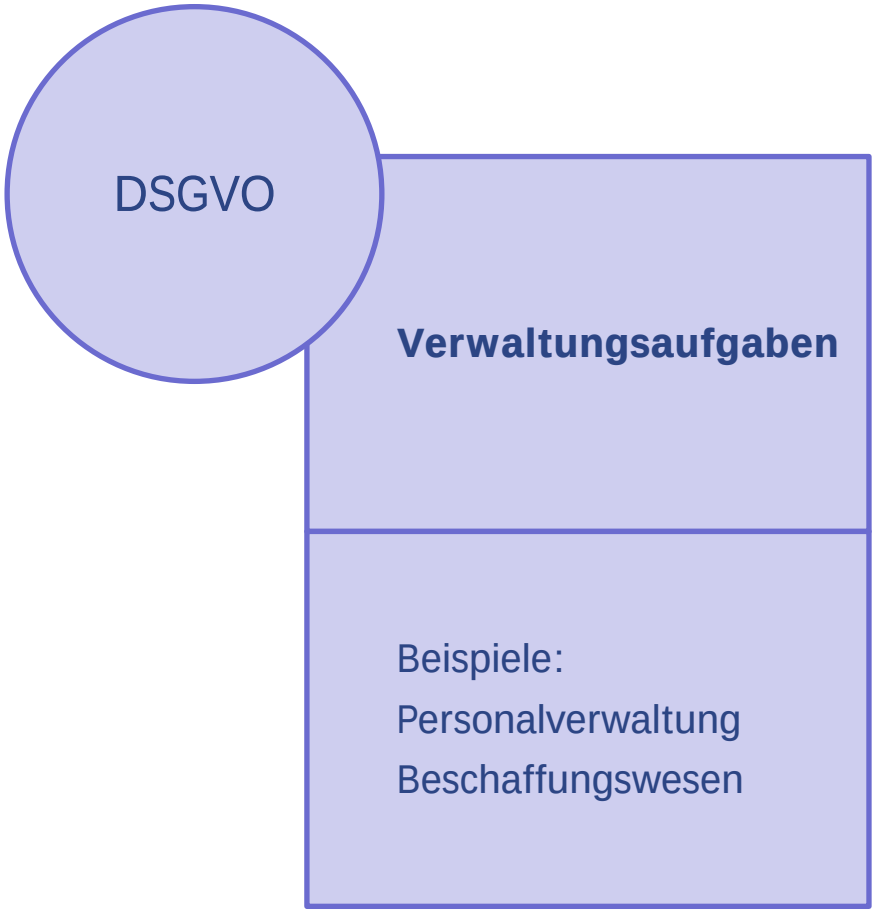
- JI-Regelungen anwendbar für alle Stellen, die für die Aufgabe Strafverfolgung zuständig sind und auch Gefahren für die öffentliche Sicherheit abwehren (Polizei).

Vollstreckung von Strafen und anderen Maßnahmen

- JI-Regelungen anwendbar für alle Stellen, die für diese Aufgaben zuständig sind, soweit sie Daten für diese Zwecke verarbeiten.

Anwendbare Vorschriften für die Polizei





Anwendbare Vorschriften für andere Behörden

JI-Regelungen	DSGVO	DSGVO
• Aufgabenerfüllung: • Verfolgung von Ordnungswidrigkeiten	• Aufgabenerfüllung: • Alle anderen Aufgaben, einschließlich Gefahrenabwehr	• Verwaltung: • Personalverwaltung • Beschaffungswesen • Etc.

WAS IST NEU NACH DER DATENSCHUTZREFORM?

Was ist neu im Datenschutzrecht?

- Wegfall der Einwilligung als Rechtsgrundlage bei Strafverfolgung und Gefahrenabwehr
- Unterscheidung nach Personen und nach Tatsachen/Einschätzungen
- Informationspflichten und Rechte der betroffenen Personen
- Benennung von behördlichen Datenschutzbeauftragten
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutz-Folgenabschätzung
- Pflichten bei „Datenpannen“
- Verpflichtung auf das Datengeheimnis
- Protokollierung von Datenverarbeitungen in Strafsachen
- Befugnisse der Landesbeauftragten für Datenschutz
- Ordnungswidrigkeiten

Einwilligung, § 27 LDSG

- DSGVO-Bereich: Einwilligung ist neben den gesetzlichen Befugnissen als Rechtsgrundlage vorgesehen. Art. 7 und Art. 8 DSGVO regeln Anforderungen an wirksame Einwilligung.
- JI-Bereich: Einwilligung ist als Rechtsgrundlage in der JI-RL nicht vorgesehen
  - Erwähnung nur in zwei Erwägungsgründen (35, 37)

    „In einem solchen Fall sollte die Einwilligung der betroffenen Person im Sinne der Verordnung (EU) 2016/679 keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen.“
  - Einwilligung nach § 27 LDSG ist dementsprechend keine eigenständige Rechtsgrundlage
  - Gemeint ist die Einwilligung nur als zusätzliche Voraussetzung zu einer gesetzlich bereits zulässigen Verarbeitung (z.B. bei DNA-Analyse).

Ausdrückliche Regelungen zu bestimmten Datenarten

- **Unterscheidung zwischen Kategorien von betroffenen Personen, § 48 LDSG**
  - Personen, z.B. Beschuldigte, Verurteilte, Geschädigte, Zeugen etc.
  - Auswirkungen, z.B. Löschfristen, Zwecke der Speicherung (z.B. Informationssystem), Zugriffsbefugnisse
- **Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen, § 49 LDSG**
  - Beurteilungen aufgrund persönlicher Einschätzungen kenntlich machen
  - Unterlagen dazu müssen bei Verantwortlichem vorhanden sein und für andere Stellen muss feststellbar sein, welche Stelle die Unterlagen führt (Aktenrückhalt)
- **Keine vergleichbare Regelung in der DSGVO**

Informationspflichten, § 31 LDSG

- DSGVO-Bereich: Artt. 13, 14 DSGVO
  - Umfangreicher Katalog an Informationen, die der betroffenen Person bei Erhebung mitzuteilen oder zur Verfügung zu stellen sind
- JI-Bereich: § 31 LDSG
  - Es sind allgemeine Informationen zur Verfügung zu stellen über
    - Zwecke der Verarbeitungen
    - Rechte der betroffenen Person (Auskunft, Berichtigung etc.)
    - Name und Kontaktdaten des Verantwortlichen und DSB
    - Anrufung und Kontakt LfD

Individuelle Benachrichtigung, § 32 LDSG

- DSGVO-Bereich:
  - Nach Art. 14 DSGVO ist grundsätzlich zu benachrichtigen, wenn Daten nicht bei der betroffenen Person erhoben wurden. Umfangreicher Katalog an Informationen.
- JI-Bereich:
  - Benachrichtigung nur, wenn dies in einer Rechtsvorschrift vorgesehen ist, z.B. nach verdeckten Ermittlungsmaßnahmen.
  - Inhalt der Benachrichtigung
    - Angaben nach § 31 LDSG
    - Rechtsgrundlage der Verarbeitung
    - Speicherdauer oder Kriterien dafür
    - Kategorien von Empfängern
    - „erforderlichenfalls weitere Informationen“

Auskunft, § 33 LDSG

- Katalog der zu beauskunftenden Daten entspricht Art. 15 Abs. 1 DSGVO. Es fehlt aber das Recht auf Kopie, das in Art. 15 Abs. 3 DSGVO enthalten ist.
- Ausnahmen von der Auskunft, etwas weiter als nach DSGVO:
  - Anders als nach § 9 Abs. 2 LDSG auch dann, wenn die Daten nur noch aufgrund von gesetzlichen Aufbewahrungsfristen gespeichert sind und nicht gelöscht werden dürfen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erforderlichen würde und Verarbeitung zu einem anderen Zweck ausgeschlossen ist.
  - Betroffene Person soll die Art der Daten näher bezeichnen, über die Auskunft verlangt wird. Möglichkeit, von der Auskunftserteilung abzusehen, wenn aufgrund fehlender Angaben unverhältnismäßiger Aufwand entsteht.

Berichtigung und Löschung, §§ 34, 50 LDSG

- Mitteilungspflichten, § 34 Abs. 5 LDSG
  - An Empfänger bei Löschung, Berichtigung oder Einschränkung der Verarbeitung
  - Bei Berichtigung außerdem an die Stellen, von denen der Verantwortliche die Daten erhalten hat
- § 50 LDSG
  - Vor Übermittlung von Daten ist deren Qualität zu prüfen
  - Außerdem bei Übermittlung Informationen beifügen, anhand derer der Empfänger die Richtigkeit, Vollständigkeit, Zuverlässigkeit und Aktualität beurteilen kann (soweit möglich und angemessen)

Benennung von behördlichen Datenschutzbeauftragten

§§ 58-60 LDSG (ähnlich wie Art. 37-39 DSGVO)

- Bestellpflicht für Behörden (Art. 37 Abs. 1 Buchst. a DSGVO und § 58 Abs. 1 LDSG für JI-Bereich). Ausnahme nur für Gerichte, die im Rahmen justizieller Unabhängigkeit handeln (§ 60 Abs. 1 S. 2 LDSG).
- Gemeinsame Bestellung eines Datenschutzbeauftragten durch mehrere Stellen möglich. Organisationsstruktur und Größe muss berücksichtigt werden.
- Datenschutzbeauftragter muss nicht zwingend Beschäftigter des Verantwortlichen sein.
- Fachkunde erforderlich im Datenschutzrecht und Datenschutzpraxis.
- Kontaktdaten müssen veröffentlicht und an LfD gemeldet werden.
- Abweichung zur DSGVO: Verschwiegenheitspflicht des DSB (§ 59 Abs. 4 LDSG und abgeleitetes Zeugnisverweigerungsrecht, § 59 Abs. 5 LDSG).

Verzeichnis von Verarbeitungstätigkeiten, § 46 LDSG (wie Art. 30 DSGVO)

- Für jede Verarbeitungstätigkeit – maßgeblich ist der Zweck der Verarbeitung, nicht das eingesetzte Mittel (z.B. „Verarbeitung von Bewerberdaten“, nicht „Einsatz von Textverarbeitungssoftware“ oder „eAkte“)
- Pflicht des Verantwortlichen
- Inhalt des Verzeichnisses, z.B.
  - Zwecke der Verarbeitung
  - Kategorien betroffener Personen und Daten
  - Kategorien von Empfängern
  - Vorgegebene Fristen für Löschung der verschiedenen Datenkategorien
  - Beschreibung der technischen und organisatorischen Maßnahmen

Datenschutz-Folgenabschätzung und vorherige Konsultation

Datenschutz-Folgenabschätzung (§ 43 LDSG, wie Art. 35 DSGVO)

- Durchführung durch verantwortliche Stelle
- Beteiligung des internen Datenschutzbeauftragten
- Bei hohem Risiko einer Verarbeitung
- Inhalt:
  - Beschreibung der Datenverarbeitung und ihrer Zwecke
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung
  - Bewertung der Risiken
  - Abhilfemaßnahmen gegen die Risiken

Datenschutz-Folgenabschätzung und vorherige Konsultation

- Wann ist eine Datenschutz-Folgenabschätzung durchzuführen?
  - Bei voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen
    - Form der Verarbeitung, insbesondere Verwendung neuer Technologien
    - Art, Umfang, Umstände und Zwecke der Verarbeitung
- „Muss-Liste“ und „Muss-nicht-Liste“ im DSGVO-Bereich
  - „Muss-Liste“, Art. 35 Abs. 4 DSGVO
    - Liste von Verarbeitungsvorgängen, für die DSFA durchzuführen ist
    - Liste veröffentlicht: https://www.datenschutzzentrum.de/dsgvo/#dsfa
  - „Muss-nicht-Liste“, Art. 35 Abs. 5 DSGVO
    - Liste von Verarbeitungsvorgängen, für die keine DSFA durchzuführen ist
    - Keine Pflicht für solche Liste
    - ULD wird keine solche Liste veröffentlichen

Datenschutz-Folgenabschätzung und Anhörung der Aufsichtsbehörde

Anhörung der LfD (§ 45 LDSG)

- Angehört wird die Datenschutzaufsichtsbehörde
- Anhörung ist erforderlich, wenn
  - aus Datenschutz-Folgenabschätzung ein hohes Risiko hervorgeht und
  - der Verantwortliche keine Maßnahmen zu dessen Eindämmung trifft.
- Verantwortliche Stelle stellt Unterlagen zur Verfügung
- Maßnahmen der Aufsichtsbehörde
  - Unterbreitung von schriftlichen Empfehlungen
  - Ausübung aufsichtlicher Befugnisse (§ 64 LDSG)

Datenschutzverletzungen, § 21 Nr. 10 LDSG (wie Artt. 33, 34 DSGVO)

- Begriff der Datenschutzverletzung: § 21 Nr. 10 LDSG
  - Verletzung der Sicherheit
  - Hat zu Vernichtung, Verlust, Veränderung oder unbefugten Offenbarung geführt
  - Personenbezogene Daten wurden übermittelt, gespeichert oder auf sonstige Weise verarbeitet
- Nicht jeder Verstoß gegen Datenschutzrecht führt zur Meldepflicht, es muss sich um eine Verletzung der Sicherheit in den genannten Ausprägungen handeln
- Relevant ist ausschließlich die objektive Verletzung der Sicherheit
  - Subjektive Momente, wie Verschulden, spielen keine Rolle
  - Ebenso ist unerheblich, wer die Verletzung verursacht hat

Pflichten des Verantwortlichen: Meldung an Aufsichtsbehörde, § 41 LDSG

- Pflichten nach § 41 LDSG
  - Meldung an die Datenschutzaufsichtsbehörde
  - Ausnahme: Die Verletzung führt nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen (z.B. verlorener Datenträger ist sicher verschlüsselt – Arbeitspapier 250 der Art. 29-Datenschutzgruppe)
  - Frist für die Meldung: unverzüglich / 72 Stunden ab Bekanntwerden der Verletzung
  - Nach Ablauf von 72 Stunden: Verzögerung der Meldung begründen
  - Auftragsverarbeiter sind verpflichtet, bekannt werdende Verletzungen unverzüglich dem Verantwortlichen zu melden

Inhalt der Meldung

- § 41 Abs. 3 LDSG
  - Beschreibung der Verletzung, mit Kategorien personenbezogener Daten, Anzahl betroffener Personen
  - Name und Kontakt des Datenschutzbeauftragten
  - Beschreibung der wahrscheinlichen Folgen
  - Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
  - Ggf. Beschreibung der Maßnahmen zur Abmilderung der möglichen nachteiligen Auswirkungen der Verletzung
- Auch schrittweise Information möglich (Abs. 4)
- Dokumentation beim Verantwortlichen (Abs. 5)

Möglichkeiten der Aufsichtsbehörde

- Prüfung, ob betroffene Personen benachrichtigt werden müssen
- Ggf. Veranlassung der Benachrichtigung, wenn Verantwortlicher diese unterlässt (§ 64 Abs. 4 LDSG in Verbindung mit Art. 58 Abs. 2 Buchst. e DSGVO)
- Prüfung, ob Maßnahmen zur Behebung der Verletzung ausreichend sind
- Prüfung, ob Maßnahmen erforderlich sind, um ähnliche Verletzungen für die Zukunft zu verhindern
- Ggf. Anordnung von Maßnahmen nach Art. 58 Abs. 2 DSGVO, § 64 LDSG
- Keine Verwendung der Meldung für Strafverfahren (nemo tenetur – § 41 Abs. 7 LDSG)

Pflichten des Verantwortlichen: Benachrichtigung der betroffenen Person(en), § 42 LDSG

- Wenn die Verletzung voraussichtlich eine erhebliche Gefahr (treffender Art. 34 DSGVO: ein hohes Risiko) für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat
- Kriterien für hohes Risiko (EG 61 JI-RL, 85 DSGVO):
  - Physischer, materieller oder immaterieller Schaden
  - Beispiele:
    - Verlust der Kontrolle über die Daten
    - Diskriminierung
    - Identitätsdiebstahl oder –betrug
    - Finanzielle Verluste
    - Rufschädigung
    - Verlust der Vertraulichkeit bei Berufsgeheimnissen

Ausnahmen von der Benachrichtigungspflicht nach § 42 LDSG

- § 42 Abs. 3 LDSG: Keine Benachrichtigung erforderlich, wenn
  - Verantwortlicher geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat (z.B. Verschlüsselung), entweder bereits im Vorfeld (Buchst. a, Nr. 1) oder nachträglich (Buchst. b, Nr. 2) oder
  - Unverhältnismäßiger Aufwand (Buchst. c, Nr. 3) – statt dessen öffentliche Bekanntmachung oder vergleichbar wirksame Maßnahme zur Information der betroffenen Personen
- § 42 Abs. 5 LDSG: Aufschiebung, Einschränkung oder Unterlassung der Benachrichtigung möglich unter den Voraussetzungen des § 32 Abs. 2 LDSG, z.B. bei Gefährdung eines Strafverfahrens.

Datengeheimnis, § 29 LDSG

- Ursprung aus dem BDSG, das Vorbild für den 3. Abschnitt des LDSG war.
- Regelung fehlt in der DSGVO, daher keine Regelung im 1. Abschnitt des BDSG und LDSG möglich.
- Datengeheimnis war bis Mai 2018 im Landesrecht SH nicht mehr enthalten, da es aufgrund der ohnehin im Beamtenrecht, im TV-L und anderer Vorschriften bestehenden Verpflichtungen für überflüssig gehalten wurde.
- Verpflichtung auf das Datengeheimnis erfolgt in der Regel schriftlich vor Beginn der Beschäftigung.

Protokollierung, § 52 LDSG

- Zu protokollierende Datenverarbeitungen
  - Erhebung, Veränderung, **Abfrage**, Offenlegung einschließlich Übermittlung, Kombination, Löschung
- Inhalt der Protokolle über Abfragen und Offenlegungen
  - Begründung für den Abruf, Datum und Uhrzeit, abfragende Person und Empfänger der Daten
- Aufbewahrungsdauer
  - Bis Ende des darauffolgenden Kalenderjahres
  - Abweichende Frist durch Spezialregelung möglich
- Übergangsfrist, § 52 Abs. 6 LDSG
  - Abweichung bis 6.5.2023 möglich
  - Für automatisierte Systeme, die vor 6.5.2016 eingeführt wurden, ...
  - ... soweit unverhältnismäßiger Aufwand besteht

Befugnisse der LfD, § 64 LDSG

- Untersuchungsbefugnisse wie bisher auch
- Anordnungsbefugnisse, § 64 Abs. 1 und 4 LDSG
  - Beanstandung
  - Warnung
  - Verwarnung
  - Anweisung, dem Antrag der betroffenen Person auf Ausübung der Betroffenenrechte zu entsprechen
  - Anweisung, Verarbeitungsvorgänge in Einklang mit Datenschutzrecht zu bringen
  - Anweisung, betroffene Personen nach einer Datenpanne zu benachrichtigen
- DSGVO-Bereich: weitergehende Befugnisse in Art. 58 Abs. 2 DSGVO (auch Verbot der Verarbeitung und Anordnung der Löschung möglich)

Ordnungswidrigkeiten bei Verstößen gegen Datenschutzvorschriften

DSGVO-Bereich

- Art. 83 Abs. 7 DSGVO: Jeder Mitgliedstaat kann selbst festlegen, ob und in welchem Umfang gegen öffentliche Stellen Geldbußen verhängt werden.
- § 19 Abs. 1 LDSG: Gegen Behörden und sonstige öffentliche Stellen werden keine Geldbußen verhängt.

JI-Bereich

- § 68 LDSG: Ordnungswidrigkeit für Verarbeitung personenbezogener Daten entgegen den Vorschriften dieses Gesetzes
- Bußgeldrahmen bis zu 50.000 Euro

Informationsmaterial

- Webseite der Datenschutzkonferenz

  https://www.datenschutzkonferenz-online.de/
- Webseite des Europäischen Datenschutzausschusses

  https://edpb.europa.eu/
- Kurzpapiere der Datenschutzkonferenz

  https://www.datenschutzzentrum.de/dsgvo/#kurzpapiere
- Vorlagen und Hinweise des ULD für das Verzeichnis von Verarbeitungstätigkeiten / Dokumentation

  https://www.datenschutzzentrum.de/dokumentation/
- Praxisleitfäden des ULD zu Einzelthemen der DSGVO

  https://www.datenschutzzentrum.de/praxisreihe/
- Datenschutz-Folgenabschätzung

  https://www.datenschutzzentrum.de/dsgvo/#dsfa
- Meldung von „Datenpannen“

  https://www.datenschutzzentrum.de/meldungen/
- Meldung von Datenschutzbeauftragten

  https://www.datenschutzzentrum.de/dsgvo/#dsb

Vielen Dank für Ihre Aufmerksamkeit

Barbara Körffer
uld5@datenschutzzentrum.de
0431 988-1216