# Auftragsverarbeitung: Aspekte aus dem Alltag

Stuttgart 25. Oktober 2018

Rudi Kramer

# Kurzvorstellung DATEV

DAS ALLES IST **DATEV**

RUND **40.300** MITGLIEDER VERTRAUEN **DATEV**

**26** NIEDERLASSUNGEN SICHERN BUNDESWEIT REGIONALE PRÄSENZ

**7** verbundene Unternehmen vertreten die DATEV in Europa

**7.400** MITARBEITER SIND FÜR DIE MITGLIEDER DER GENOSSENSCHAFT TÄTIG

SIE ERZIELTEN 2017 EINEN UMSATZ VON **978** MILLIONEN EURO

# Agenda

- **Basics**
  - Form
  - anderen Rechts-instruments
  - Inspektions-recht
  - Abgrenzungen
- **Besonderheiten**
  - Einbindung von Experten
  - Wartung
- **offene Fragestellungen**
  - „Öffnungs-klauseln“?
  - Fehleranalyse

# Anforderungen an die Form

## Abschluss auch in elektronischer Form, Art. 28 (9) DS-GVO

Elektronisches Format → Anwendung der Regelungen des BGB (§ 126a → qualifiziert elektronische Signatur)?

<u>Antwort der EU-Kommission auf eine Anfrage im Europäischen Parlament</u>:

*"It is not necessary to append an electronic signature to contracts for them to have legal effects. E-signatures are one of several means to prove their conclusion and terms."*

➔ Elektronische Signatur ist nicht erforderlich. Ausschlaggebend ist, dass die Nachweisfähigkeit der Vereinbarung (zwei übereinstimmende Willenserklärungen) gegeben ist.

➔ **Ergebnis:**

Vertragsabschluss auch über automatisierte Vertragsprozesse E-Mail/online (z. B. Klickboxen) möglich, er muss nur nachweisbar sein.

# … anderen Rechtsinstruments …

… auf Basis eines Vertrages oder eines anderen Rechtsinstruments der Europäischen Union oder der Mitgliedsstaaten, Art. 28 (3) Satz 1 DS-GVO.

Der Begriff des Rechtsinstruments wird nicht näher definiert.

Kommentare gehen auch davon aus, dass damit Gesetze und Verordnungen gemeint sein können.

Antwort der EU-Kommission auf eine Anfrage im Europäischen Parlament:

*"A legal act may be an ordinance or other type of administrative decision whereby controllers vested in public authority may stipulate the conditions for processing personal data on their behalf."*

➔ **Ergebnis:**

Ein Rechtsinstrument wäre danach irgendeine Art von Verwaltungsentscheidung, mit welcher der Verantwortliche (in der Regel eine öffentliche Stelle) die Bedingungen für die Verarbeitung personenbezogener Daten in seinem Namen festlegen kann. Ein Gesetz wird dafür nicht verlangt.

# Inspektionsrecht

## BayLfD https://www.datenschutz-bayern.de/datenschutzreform2018/aki06.html :

Der Bayerische Landesbeauftragte
für den Datenschutz

- Inspektionsrecht vor Ort durch Auftragsverarbeiter ist kostenlos zu gewähren — keine nachträgliche Regelung zu Entgeltpflicht zu treffen
- Interesse des Auftragsverarbeiters kann durch „Einpreisen“ von vornherein gewahrt werden

- Beachte: DS-GVO gibt für kostenlose Leistungen keine Begründung, nicht jede Aufgabe, die das Gesetz vorsieht, muss umsonst erbracht werden
  - Inspektionsrecht darf nur nicht durch „Mondpreise“ ausgehebelt („Abschreckung“) werden, aber eine verursacherbezogene Zuordnung ist nicht ausgeschlossen.
  - Empfehlung: dies in jedem Fall vor Vertragsschluss zu klären!

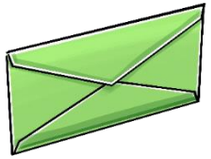
  - Im Übrigen: Umkehrschluss würde bei einem externen DSB dazu führen, dass seine Unterstützung auch nicht verursacherbezogen abgerechnet werden dürfte, sondern jegliche Beratung und Unterstützung von vornherein „eingepreist“ werden müsste.

# Abgrenzungen

## Wann liegt keine Auftragsverarbeitung vor?

<u>Kurzpapier Nr. 13 der Datenschutzkonferenz</u>:

- Anhang B: Inanspruchnahme fremder Fachleistung, die eigenständig erbracht werden
  - Berufsgeheimnisträger (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer)
  - Inkassobüro mit Forderungsübertragung
  - Bankinstitute für den Geldtransfer
  - Postdienste für den Brieftransport
  - ... und vieles mehr ...



# Abgrenzungen

## Wann liegt keine Auftragsverarbeitung vor?

<u>Kurzpapier Nr. 13 der Datenschutzkonferenz</u>:

- Anhang C: gemeinsame Verantwortlichkeit
  - klinische Arzneimittelstudien, wenn mehrere Mitwirkende (z. B. Sponsor, Studienzentren/Ärzte) jeweils in Teilbereichen Entscheidungen über die Verarbeitung treffen
  - gemeinsame Verwaltung bestimmter Datenkategorien
    z. B. „Stammdaten“ für bestimmte gleichlaufende Geschäftszwecke mehrerer Konzernunternehmen
  - vgl. auch <u>Kurzpapier Nr. 16 zur gemeinsamen Verantwortlichkeit</u>

# Abgrenzungen

## Wann liegt keine Auftragsverarbeitung vor?

Bayerisches Landesamt für
Datenschutzaufsicht

**<u>FAQ des BayLDA zur DS-GVO</u>**:

**Inanspruchnahme fremder Fachleistungen bei einem eigenständigen Verantwortlichen:**

- Tätigkeiten der Berufsgeheimnisträger (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer)
- Inkassobüros mit Forderungsübertragung
- Bankinstitute für den Geldtransfer
- Postdienste für den Brief- oder Pakettransport
- Tätigkeit als WEG-Verwalter
- Detektive bei ihrer Observierungs-/Überwachungs-/Ausforschungstätigkeit
- beauftragte Warenzusendung:
  - Hersteller und Großhändler, die von Einzelhändlern für mit Endkunden vereinbarte Direktlieferungen die Endkundenadressen erhalten
  - Blumen- oder Weinversender, die eine Liste mit Adressdaten zur Versendung der Blumen- bzw. Weingeschenke an dritte Personen erhalten

# Abgrenzungen

## Wann liegt keine Auftragsverarbeitung vor?

Bayerisches Landesamt für
Datenschutzaufsicht

**Inanspruchnahme fremder Fachleistungen bei einem eigenständigen Verantwortlichen:**

- Insolvenzverwalter
- Personalvermittlung nach Auftrag von Stellensuchenden oder Arbeitgebern
  (siehe dazu auch Beispiel 6 im WP 169)
- Internet-Plattformbetreiber zur Vermittlung zwischen Anbietern und Nachfragern, die sich auf der Plattform treffen können
- TKG-Dienstleistungen, es sei denn, darüber hinausgehende Zusatzdienste wie Auslagerung einer betrieblichen Telefonanlage oder Cloud-Speicherlösungen usw.
  (siehe dazu auch Beispiel 1 im WP 169)
- Versicherungs-/Finanzmakler, -vermittler im Rahmen des Kundenvertrags
- Handelsvertreter im Rahmen ihrer Beratungstätigkeit und Vertragsvermittlungen
- Übersendung von Schulungsteilnehmer-Daten zur Durchführung der Schulung an einen externen Trainer, Schulungsveranstalter oder an das Tagungshotel

# Abgrenzungen

## Wann liegt keine Auftragsverarbeitung vor?

Bayerisches Landesamt für
Datenschutzaufsicht

**Inanspruchnahme fremder Fachleistungen bei einem eigenständigen Verantwortlichen:**

- Fertigung individueller medizinischer Produkte, Hilfsmittel, Prothesen etc. für Patienten/Kunden im Auftrag von Ärzten, Zahnärzten, Apotheken, Sanitätshäusern usw.
- medizinische Labore, Materiallabore usw. (Materialuntersuchung im Auftrag)
- Zahlungsdienstleister für elektronische Zahlungen (Transport von Zahlungsdaten, Geldwäsche- und Betrugsprüfung nach ZAG (Gesetz über die Beaufsichtigung von Zahlungsdiensten) und den Mindestanforderungen der BaFin)
- von Reisebüros aufgrund Kundenvertrags vermittelte Leistungsanbieter, wie Hotels, Mietwagenfirmen, Fluggesellschaften, Busunternehmen, Versicherungen usw. (siehe dazu auch Beispiel 8 im WP 169).

➔ **Anforderungen an beauftragendes Unternehmen:**
Je nach Sachverhalt sind vom Verantwortlichen ggf. Zweckbindung und Vertraulichkeit zu den dabei berührten personenbezogenen Daten festzulegen.

# Abgrenzungen

## Wann liegt keine Auftragsverarbeitung vor?

Bayerisches Landesamt für
Datenschutzaufsicht

**Keine Auftragsverarbeitung, wenn Tätigkeit im Kern keine beauftragte Verarbeitung personenbezogener Daten, sondern der Auftrag zielt auf eine andere Tätigkeit:**

- vom Vermieter beauftragte Handwerker, die dazu die nötigen Mieterdaten erhalten
- Sachverständige zur Begutachtung eines Kfz-Schadens
- Personenbeförderung, Krankentransportleistungen
- Bewachungsdienstleistungen
- Reinigungsdienstleistungen und Handwerkereinsätze in Unternehmen
- Reinigung von Berufskleidung mit Namensschildern

# Abgrenzungen

## Wann liegt keine Auftragsverarbeitung vor?

Bayerisches Landesamt für
Datenschutzaufsicht

**Keine Auftragsverarbeitung, wenn Tätigkeit im Kern keine beauftragte Verarbeitung personenbezogener Daten, sondern der Auftrag zielt auf eine andere Tätigkeit**:

- Druck von Prospekten, Katalogen, mit Bildern von Beschäftigten oder Fotomodellen
- Transport von ausreichend geschreddertem Papiermaterial
- Transport von Unterlagen und Waren durch Kurierdienste, Speditionen, Zeitungsausträger
- Übersetzung von Texten in/aus Fremdsprachen

➔ **Anforderungen an beauftragendes Unternehmen:**
Je nach Sachverhalt sind vom Verantwortlichen ggf. Zweckbindung und Vertraulichkeit zu den dabei berührten personenbezogenen Daten festzulegen.

# Agenda

**Basics**
- Form
- anderen Rechts-instruments
- Inspektions-recht
- Abgrenzungen

**Besonderheiten**
- Einbindung von Experten
- Wartung

**offene Fragestellungen**
- „Öffnungs-klauseln“?
- Fehleranalyse

# Einbindung von Experten

## Kurzpapier der DSK Nr. 13

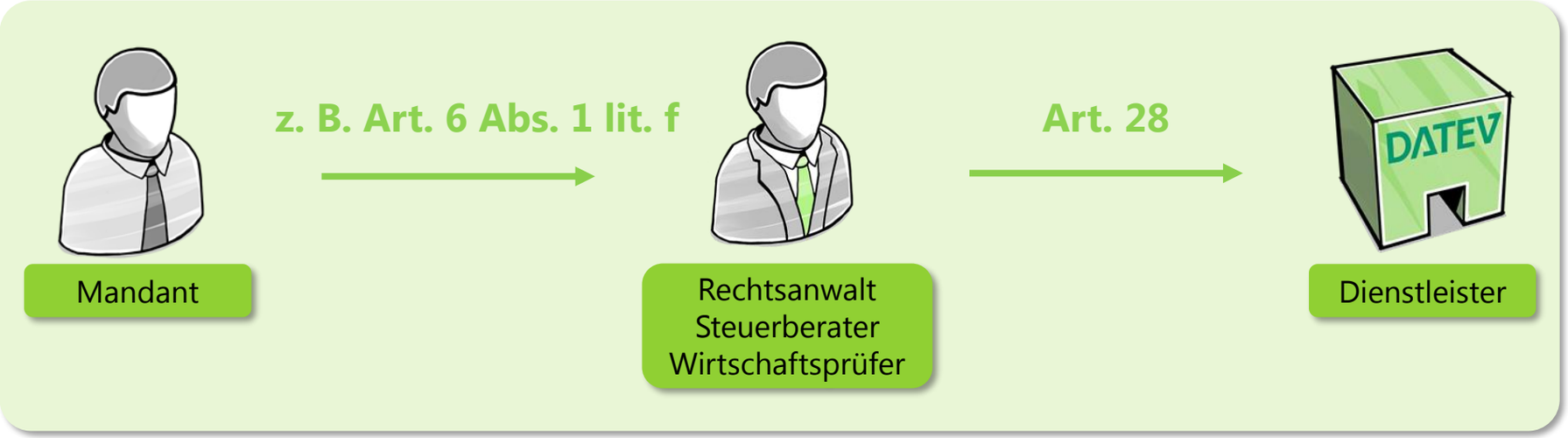
- Es gibt auch Beauftragungen, die keine Auftragsverarbeitungen sind, z. B. Berufsgeheimnisträger, Postdienstleistung etc. (Anhang B).
- Rechtmäßigkeitsgrundlage ist in Art. 6 zu suchen.
  - z. B. Art. 6 (1) lit. f bei der Mandatierung eines Rechtsanwalts oder Steuerberaters.
- (Wieder mal) **Diskussion**, ob dies auch bei der Mandatierung des Steuerberaters mit der Beratung zur Lohn- und Gehaltsabrechnung gilt, wenn dabei auch die Gehaltsabrechnung erstellt wird.
  - **LDI NRW**: Die technische Teilleistung ist getrennt zu betrachten.
  - **BayLDA**: Maßgeblich ist der erteilte Beratungsauftrag, technische Erstellung von Ergebnissen kann nicht getrennt werden.
  - **BStBK**: Leistungsgebiet des Steuerberaters ist die Beratung, die unabhängig, eigenverantwortlich (weisungsfrei), gewissenhaft und verschwiegen durchzuführen ist.
    Eine weisungsabhängige Leistungserbringung führt zu berufsrechtlichen Konsequenzen.
  - **Gesetzgeber**: Lohn- und Gehaltsabrechnung ist inkludierter Teil der unbeschränkten Hilfeleistung in Steuersachen (Umkehrschluss aus § 6 Nr. 4 StBerG), auch wird in der Steuerberatervergütungsverordnung keine Differenzierung vorgesehen (§ 34 StBVV).

# Einbindung von Experten

## Welche Grundlagen können dabei herangezogen werden?

Neben Art. 6 (1) lit. f kommen in Betracht:

- Art. 88 i.V.m. § 26 Abs. 1 Satz 1 i.V.m. Abs. 3 bei der Mandatierung des Steuerberaters mit Beratung zur Gehaltsabrechnung der Beschäftigten (inkl. Erstellung der Lohn- und Gehaltsabrechnung), zu Berechnungen und Entscheidungen zur betrieblichen Altersversorgung, etc.
- Art. 9 (2) lit. f bei der Mandatierung eines Rechtsanwalts zur Rechtsverfolgung.
- Art. 9 (2) lit. g bei der Mandatierung eines Steuerberaters mit Leistungen nach dem StBerG.
  - Verarbeitung auf der Grundlage des Rechts eines Mitgliedsstaates (→ StBerG, insb. § 11 StBerG).
  - Steht in angemessenem Verhältnis zu dem verfolgten Ziel (→ Art. 9-Daten nur als wirtschaftliche Information).
  - Angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person (→ berufsrechtliche Pflichten, vgl. § 32 II, § 57 I StBerG, inkl. Strafbarkeit nach § 203 StGB).
  - Aus Gründen eines erheblichen, öffentlichen Interesses (→ besonderes Berufsrecht, um Qualität der Steuer- und Abgabenprozesse sicherzustellen).

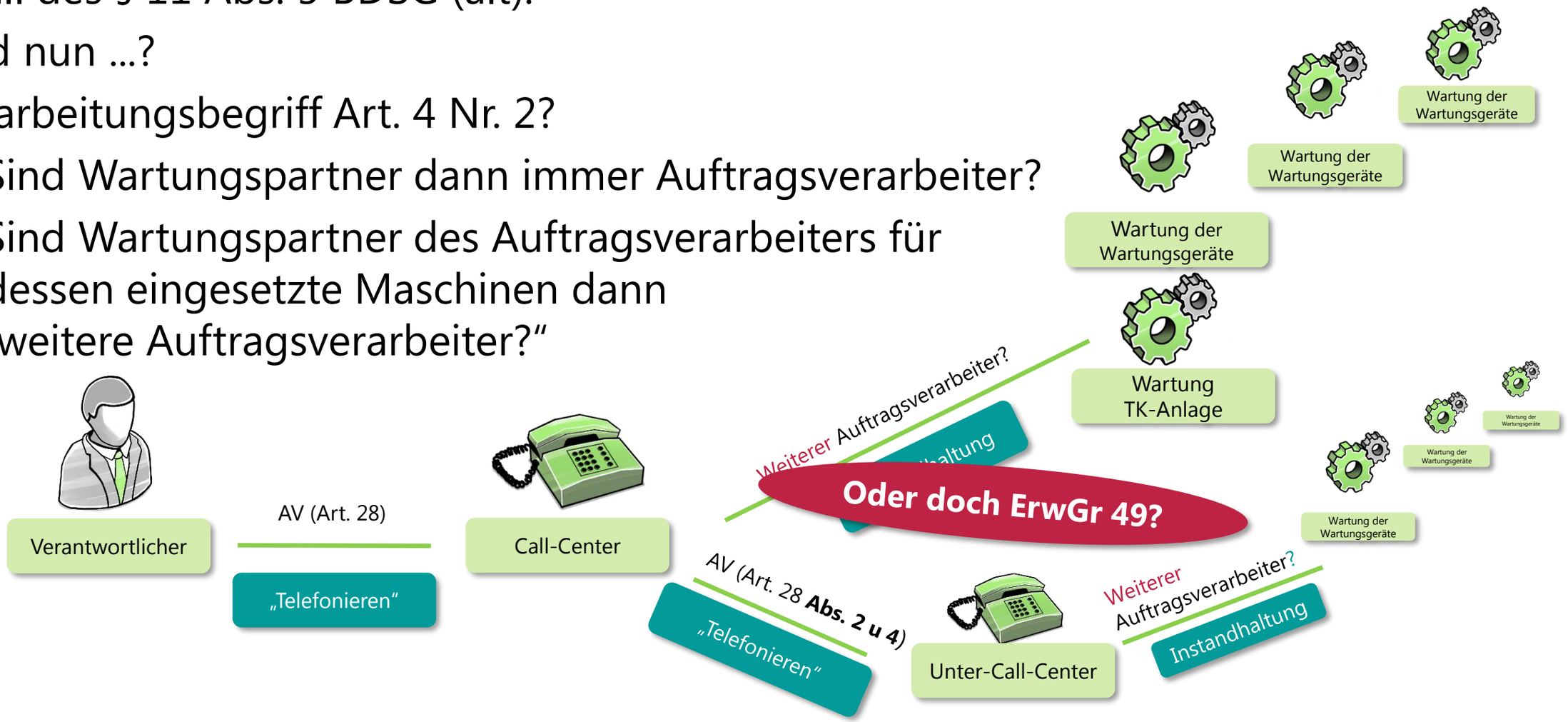



| (freie Berufsausübung, Leistung in Berufsordnung geregelt) | Auftragsverarbeitung |
|---|---|
| Art. 6 Abs. 1 lit. f DS-GVO<br>Art. 88 DS-GVO i.V.m. § 26 I 1, III BDSG<br>Art. 9 (2) lit. g DS-GVO<br>Art. 9 (2) lit. f DS-GVO | Art. 28 DS-GVO |

# Wartung

Wegfall des § 11 Abs. 5 BDSG (alt).

- Und nun …?
- Verarbeitungsbegriff Art. 4 Nr. 2?
  - Sind Wartungspartner dann immer Auftragsverarbeiter?
  - Sind Wartungspartner des Auftragsverarbeiters für dessen eingesetzte Maschinen dann „weitere Auftragsverarbeiter?“



# Wartung

## Was ist Wartung?

- Definition: Einspielen von Daten, Konvertierung, Abgleichen, aber auch Aktualisierung durch Patches, Updates.

- DSK in Kurzpapier Nr. 13: Wartung/Fernwartung → Verarbeitungsbegriff → Auftragsverarbeitung

→ **ErwGr. 49:**

Grundlage der Verarbeitung bei Störungen und Einbeziehung von externen Spezialisten auch Art. 6 (1) lit. f.

Die Verarbeitung von pbD stellt ein berechtigtes Interesse dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist.

→ Mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder mutwillige Eingriffe abzuwehren, die geeignet sind, Anforderungen an Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit beeinträchtigen.

# Agenda

**Basics**
- Form
- anderen Rechts-instruments
- Inspektions-recht
- Abgrenzungen

**Besonderheiten**
- Einbindung von Experten
- Wartung

**offene Fragestellungen**
- „Öffnungs-klauseln“?
- Fehleranalyse

# Öffnungsklauseln bei der Auftragsverarbeitung

## Gibt es welche?

Möglichkeiten für Mitgliedsstaaten zur Gestaltung:

- z. B. Art. 28 (3) lit. a (→ eEvidance)
- z. B. Art. 29 (Weisungsgebundenheit, es sei denn Verpflichtung nach dem Recht des Mitgliedsstaates zur Verarbeitung)
- z. B. § 20a Finanzverwaltungsgesetz (weitere Anforderungen an Auslagerung)
- z. B. § 80 II SGB X (z. B. Voraussetzungen für Auslagerung, Einschränkung nach Art. 49 (5))

- DSK in Kurzpapier Nr. 13: Wartung/Fernwartung → Verarbeitungsbegriff → Auftragsverarbeitung

→ **Regelungen in Art. 28 sind daher nicht (so richtig) abschließend,**
allerdings auch nur da, wo DS-GVO den Mitgliedsstaaten eine Regelungsbefugnis zuweist!

# Öffnungsklauseln bei der Auftragsverarbeitung

## Wartung

Woher nimmt Gesetzgeber die Befugnis, in Spezialgesetzen etwas zur „Wartung zu regeln“, wenn sich dies doch schon aus der Definition „Verarbeitung“ ergeben sollte?

- Absatz in Landesdatenschutzgesetze regelt dies extra, wie in Art. 5 Abs. 3 BayDSG;

- Kirchl. Datenschutzrecht:
  § 29 KDG: Abs. 12: bei Wartung gilt Auftragsverarbeitung entsprechend, Abs. 11: Drittstaat nur bei Angemessenheitsbeschluss, Abs. 5: weitere Auftragsverarbeitungen sind auch auf KDG zu verpflichten, Abs. 9: elektr. Format nur nach § 126 ff BGB,
  § 57 KDG: Anpassungsfrist bisheriger Auftragsverarbeitung bis 31.12.2019
  DSG-EKG: § 30 Abs. 5: → Art. 28 DS-GVO, wenn Auftragnehmer nicht dem DSG-EKG unterliegt.

- § 80 V SGB X (Ausnahme, wenn es sich um Wartung handelt.)

# Fehleranalyse

## Ist Fehleranalyse immer als Auftragsverarbeitung zu behandeln?

Oder müsste differenziert werden, wenn es sich um Fehleranalyse handelt:

- ✓ ErwGr. 49, der Dienstleister entscheidet selbst, welche Maßnahmen er durchführt, um die Abwehr/Beseitigung von Störungen sicherzustellen.
- ✓ pbD sind nicht Kernbereich des Auftrags, sondern können nur nicht vermieden werden, vgl. Abgrenzung durch BayLDA.
- ➔ Grundlage: Wahrung berechtigter Interessen, Art. 6 (1) lit. f
  - ➔ Betroffenenrechte: Art. 14 (5) lit. b, bzw. Anwendungsbereich des Art. 11 zu prüfen

- und Daten nach Art. 9?
  Dort keine Verarbeitung aufgrund Wahrung berechtigter Interessen möglich?
  → teleologische Reduktion → verarbeitungskontextsensitive Auslegung.
  Eine Verarbeitung im Rahmen einer Fehleranalyse, die in Hinblick auf die besondere Sensitivität der Datenkategorien vollkommen neutral ist, führt dazu, dass sich aus deren Verarbeitung gerade keines der vom Verordnungsgeber für die gesteigerte Schutzbedürftigkeit dieser Datenkategorien unterstellten Risiken realisiert.

# Ausblick

- Einigung der Datenschutzkonferenz hinsichtlich der Mandatierung von Steuerberatern?
- Differenzierung bei der Einbeziehung von Sicherheitsexperten bei Fehleranalyse/ Fehlerbehebung gem. ErwGr. 49 als „Wahrung berechtigter Interessen“?
- Teleologische Reduktion bei der Verarbeitung besonderer Kategorien gem. Art. 9 (2), ErwGr. 56, um die Beauftragung von externen Fachexperten für Fehleranalysen zu ermöglichen?

DATEV

Zukunft gestalten. Gemeinsam.

© DATEV eG, alle Rechte vorbehalten