DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

# Mehr Rechtssicherheit durch Verhaltensregeln: Beispiel Trusted Data Processor

Dr. Niels Lepperhoff

# 5 Jahre Anwendung der DS-GVO…

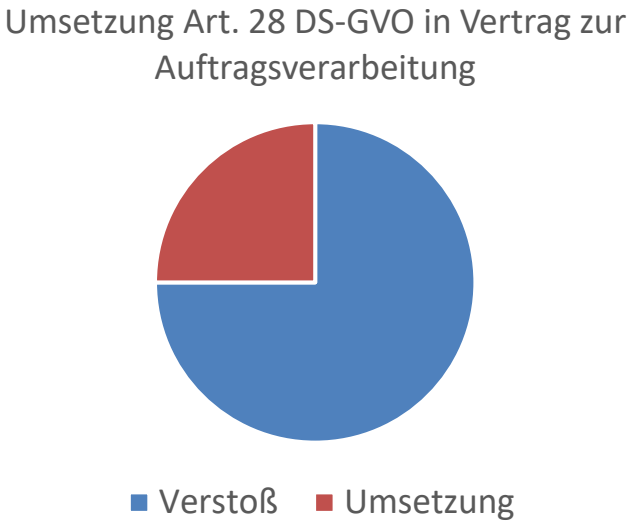
… mit ernüchternder Erfahrung

Beispiel Auftragsverarbeitung

- 75% geprüfter Auftragsverarbeitungsverträge verstoßen gegen Art. 28 DS-GVO

  (Erfahrung der Xamit Bewertungsgesellschaft mbH aus Prüfung von 48 Verträgen 01/2020 bis 09/2023, die 8 Kunden zur Prüfung vorgelegt haben)

- Folgen
  - Zusätzliche Aufwände für Verhandlung ➔ Verhandlungskosten ggf. höher als Leistungswert
  - Teilweise: Dienstleisterwechsel
- Eindruck bei Entscheidern
  - Beauftragung von Auftragsverarbeitern = aufwändig + frustrierend



# Vollzugsdefizit und Wettbewerbsnachteile

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Gewünscht – doch im Moment nicht gegeben
  - Vertrauen, dass Auftragsverarbeiter DS-GVO einhält
- Folgen
  - Hohe Prüf- und Korrekturaufwände bei Auftraggebern
  - Wettbewerbsnachteile für Auftragsverarbeiter mit korrekter Umsetzung der DS-GVO
- Selbsthilfe der deutschen Wirtschaft
  - Verhaltensregel Trusted Data Processor
    - Rechtssicherheit schaffen
    - Compliance-Kosten zur Beauftragung senken

# WAS IST EINE VERHALTENSREGEL?

# Zielsetzung: „Verhaltensregel“

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

**DS-GVO**

Abstrakte Anforderungen

**Verhaltensregel**

Übersetzung in Prozesse, konkrete Handlungen

**Selbstverpflichtung auf Verhaltensregel**

| Nachweis der Einhaltung | Sichtbare Compliance |
|---|---|

# Wirkungen nach DS-GVO

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

| | |
|---|---|
| Dokumentations-erleichterungen | • Nachweis der Einhaltung verschiedener Normen (Artt. 24, 28 (1) + (4), 32 (1))<br>• Berücksichtigung bei DSFA (Art. 35 (8)) |
| Datenschutzniveau im Drittland | • Mittel zum Heben des Datenschutzniveaus (Art. 46 (2) e))<br>• gilt nur, wenn Verhaltensregel dieses Ziel verfolgt |
| Bußgeldhöhe | • Senkende Wirkung möglich (Art. 83 (2) j)) |

# Weg zur Genehmigung

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

**Einreichung einer Verhaltensregel zur Genehmigung**

| durch Verband, Verein | bei der zuständigen Datenschutzaufsichtsbehörde |
|---|---|

**Antragstellung zur Akkreditierung einer Überwachungsstelle (nicht-öffentliche Stellen)**

| durch Überwachungsstelle | Bei der zuständigen Datenschutzaufsichtsbehörde |
|---|---|

**Genehmigung der Verhaltensregel & Akkreditierung der Überwachungsstelle**

durch zuständige Datenschutzaufsichtsbehörde

# Prüfungen im Rahmen der Genehmigung

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

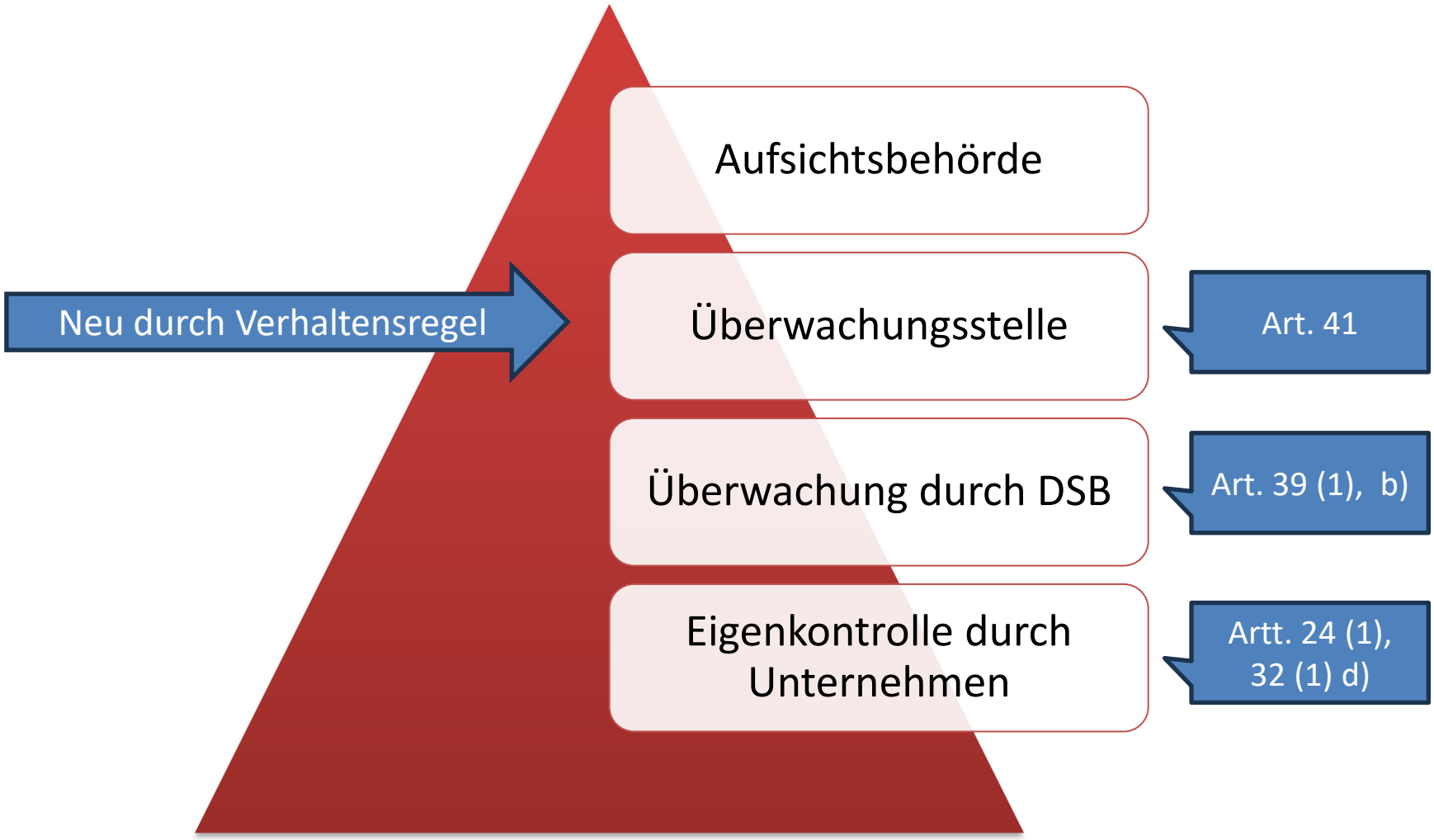
| | |
|---|---|
| Konkretisierung | • Keine Wiederholung gesetzlicher Vorgaben<br>• Jede Regelung muss DS-GVO konkretisieren (Verständnis in DE) |
| Über DS-GVO hinausgehen | • Streiche alle Regelungen ohne Verankerung in DS-GVO<br>• Kein „Sahnehäubchen“ erlaubt |
| Existiert Überwachungsstelle | • Genehmigungsvoraussetzung für Anwendung auf nicht-öffentliche Stellen |

# Aufgaben Überwachungsstelle

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

| | |
|---|---|
| Überwachung Einhaltung | • Regelmäßige Überwachung der Einhaltung<br>• Anlassbezogene Kontrollen |
| Beschwerde-bearbeitung | • Entgegennahme von Beschwerden<br>• Sachverhaltsermittlung |
| Sanktionen | • Ergreifen von Maßnahmen bei Nichtbefolgung der Verhaltensregel |

# Erweiterung der Kontrollpyramide



# Voraussetzung für Wirkung

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

**Sich orientieren**

- Wirkungen aus DS-GVO finden *keine* Anwendung
- Unverbindlich

**Selbstverpflichtung**

- Wirkungen aus DS-GVO finden Anwendung
- Verbindlich durch Vertrag o.ä.
- Überwacht durch Überwachungsstelle

# Anwendungsbereiche

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

| | |
|---|---|
| Deutschland (Option 1) | • Genehmigung & Akkreditierung durch deutsche Aufsichtsbehörde |
| EU (Option 2) | • Genehmigung durch nationale Aufsichtsbehörde UND Europäischen Datenschutzausschuss<br>• Akkreditierung durch nationale Aufsichtsbehörde |
| Verbindliche Anwendung in EU (Add-on zu Option 2) | • Verbindlichkeitsbeschluss einer genehmigten Verhaltensregel durch EU-Kommission |

# Rechtssicherheit durch Verhaltensregeln

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

**Inhaltliche Prüfung durch Aufsichtsbehörde**

Konkretisierung bestehender Anforderungen aus DS-GVO

**Genehmigung durch Aufsichtsbehörde / Europ. Datenschutzausschuss**

Verbindliche Bestätigung: Konkretisierung setzt DS-GVO um

**Rechtssicherheit entsteht**

Voraussetzung: Umsetzung Verhaltensregel UND
handeln im Geltungsbereich der Verhaltensregel

# Verhaltensregel vs. Zertifizierung 1/2

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

| | Verhaltensregel | Zertifizierung |
|---|---|---|
| Geregelt in | Art. 40 | Art. 42 |
| Ziel | Konkretisieren & Einhaltung nachweisen | Einhaltung nachweisen |
| Verfahren | Inhaltliche Genehmigung Akkreditierung Überwachungsstelle | Genehmigung Kriterien Akkreditierung Zertifizierungsstelle durch DAkkS oder Aufsichtsbehörde |
| Zuständig | Nationale Aufsichtsbehörde / EDPB | Nationale Aufsichtsbehörde / EDPB |
| Einreicher | Verein, Verband | Zertifizierungsstelle |

# Verhaltensregel vs. Zertifizierung 2/2

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

| | Verhaltensregel | Zertifizierung |
|---|---|---|
| Nachweis Einhaltung Art. 24 | ✓ | ✓ |
| Nachweis für AV Art. 28 (1), (4) | ✓ | ✓ |
| Nachweis Einhaltung Art. 32 (1) | ✓ | ✓ |
| Berücksichtigen DSFA Art. 35 | ✓ | ✗ |
| Datenschutzniveau Drittstaat Art. 46 (2) e) | ✓ | ✓ |
| Bußgeldreduktion Art. 83 (2) j) | ✓ | ✓ |
| Kontrolle Einhaltung | Regelmäßige Prüfung | Prüfung mind. alle 3 Jahre |
| Beschwerde & Sanktion | ✓ | ✓ |
| Konkrete Umsetzung DS-GVO | ✓ | ✗ |

# TRUSTED DATA PROCESSOR

# DS-GVO: Delegation Prüfen & Sicherstellen an Auftraggeber

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

**Auswahl**

- Auswahl von Auftragsverarbeitern mit „Garantie“ zur Einhaltung DS-GVO (Art. 28 (1))
- Verhaltensregel = heranziehbar als Teil einer „Garantie“

**Vertragsgestaltung**

- „Malen nach Zahlen“: Vertragsparteien müssen Regelungsziele umsetzen (Art. 28 (3))
- Umsetzungsweg: offen

**Sicherstellungspflicht**

- Sicherstellen und Nachweisen DS-GVO konforme Verarbeitung auch beim Auftragsverarbeiter (Art. 24 (1))

# Auftragsverarbeitung = enges Zusammenwirken

# Ausgangslage

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Auftragsverarbeitung = teures Vergnügen

- Genereller Eindruck
  - Umsetzung gesetzlicher Anforderung nicht selbstverständlich
- Vertrag zur Auftragsverarbeitung (AVV)
  - Häufig Verhandlungsbedarf
- Leistungserbringung
  - Prüfbedarf
- Vertragslaufzeit
  - Erforderlichkeit zur regelmäßigen Prüfung → gilt auch bei Leistungen von 10 €/Monat

# Trusted Data Processor: Zielsetzung

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

# Nutzen aus Sicht der Auftraggeber

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

**Einfachere Vertragsprüfung & Verhandlung**

- Häufige Streitpunkte in AVV geregelt (Kontrollrechte, UAN)
- Auszutauschende Informationen in Umfang und Zeitpunkt festgelegt

**Geringerer Kontrollbedarf**

- Für Auftraggeber wichtige Prozesse im Detail vorgegeben = Transparenz
- Eigenkontrolle mit Vorgabe Inhalt
- Überwachung durch DSZ

# Nutzen aus Sicht der Auftragsverarbeiter

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

| | |
|---|---|
| Einfachere Vertragsprüfung & Verhandlung | • Häufige Streitpunkte in AVV geregelt<br>• Abwehr überschießender Auftraggeberwünsche |
| Standardisierter Kontrollbedarf | • Ein Prüfbericht für alle Auftraggeber |
| Rechtssicherheit | • Bei Prozessen, AVV-Klauseln, Vertraulichkeitsverpflichtung |
| Sichtbare Compliance | • Werbung mit „Gesetzestreue“ „problematisch“<br>• Ausweg: Werbung mit Selbstverpflichtung |

# STANDARDISIERUNG AM BEISPIEL

# Beispiel: Transparenz & Kontrollrechte

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Probleme in der Praxis
  - Unterauftragnehmer (UAN) erst in AVV offen gelegt → teilweise Leistungsvertrag bereits unterzeichnet
  - Einschränkung der Kontrollrechte in AVV
- Lösung
  - Nennung UAN in Angebot
  - Vorgegebenes Mindestniveau in AVV zu Kontrollrechten des Auftraggebers

# Beispiel: Kontrolle & Datenschutzprozesse

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Probleme in der Praxis
  - Auftraggeber: Muss viele Auftragsverarbeiter kontrollieren
  - Auftragsverarbeiter: 1 andere Checkliste pro Auftraggeber
- Lösung
  - Standardisierung von Datenschutzprozessen mit Relevanz für Auftraggeber
  - Vorgaben zur Eigenkontrolle inkl. Bericht an Auftraggeber
  - Vorgaben zur Kontrolle Unterauftragnehmer

# Beispiel: Kommunikation

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Probleme in der Praxis
  - Weisungsberechtigte/Weisungsempfänger und weitere Ansprechpartner sind unbekannt
- Lösung
  - Rechtzeitige Kommunikation der relevanten Ansprechpartner und der Kontaktdaten

# Übersicht der Vorgaben beim Auftragsverarbeiter

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

# EINFACH MITMACHEN

# Wer kann sich selbstverpflichten?


Hinweis: Sitz und Ort der Verarbeitung von Unterauftragsverarbeitern = unerheblich

# Einfache Einführung

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

1. 
   - Trusted Data Processor herunterladen (verhaltensregel.eu/verhaltensregel/)
2. 
   - Vorgaben umsetzen
3. 
   - Antrag stellen unter verhaltensregel.eu/antrag/

# Einführungsaufwand

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Vorteil

- Keine über DS-GVO hinausgehende Anforderungen

Anpassungsbedarf

- Angebot & AVV anpassen
- 4 vorhandene Prozessbeschreibungen anpassen
- Verpflichtung auf Vertraulichkeit bei Abweichungen ggf. neu einholen
- Konzeption der Eigenkontrolle und der Kontrolle der Unterauftragsverarbeiter

} Ca. 4-8 Stunden

# Umgang mit Altverträgen

- Entscheidung des Unternehmens
  1. Umstellung auf neue AVV = Kunden profitieren von Trusted Data Processor
  2. Keine Umstellung auf neue AVV = Trusted Data Processor gilt für diese Kunden nicht

# Kontakt

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Sprechen Sie uns an

- vertrieb@verhaltensregel.eu
- 030 / 754 391 597
- kostenlose Beratung