DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Informationen zur Verhaltensregel „Trusted Data Processor“

Stephan Rehfeld, Vorstand BvD

Dr. Niels Lepperhoff, DSZ

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

WAS IST EINE VERHALTENSREGEL?

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

Vorteile einer Verhaltensregel

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Grundsatz: Beitrag zur ordnungsgemäßen Anwendung der DS-GVO
  => besondere Bedürfnisse von Kleinstunternehmen und KMU
- Wirkungen aus DS-GVO
  - Dokumentationserleichterungen
  - Angemessenes Datenschutzniveau beim Empfänger im Drittland
  - Positiver Einfluss auf Bußgeldbemessung
- Zusätzliche Wirkung
  - Rechtssicherheit durch Konkretisierung in Verhaltensregel
  - Überwachte Einhaltung durch Überwachungsstelle

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

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

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

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	✓	×

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

WAS MACHT „TRUSTED DATA PROCESSOR“?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Trusted Data Processor: Zielsetzung

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Konkretisierung der DS-GVO Anforderung

Auftraggeber

Auftragsverarbeiter

Transparenz

Datenschutz-prozesse

Kontroll-erleichterung

Mittel: Standardisierung durch verbindliche Vorgaben

Relevant für alle Unternehmen in DE

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

WAS WAREN UND SIND DIE ROLLEN DES BVD UND DER GDD?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Ausgangslage seit 2011

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Auftragsverarbeitung = teures Vergnügen

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

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

Grundlagen & Impulse

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

BvD & GDD

- Vorarbeiten & Impulse
- Rückkopplung mit der Praxis
- Inhaltliche und organisatorische Unterstützung bei Verhandlungen
- Startfinanzierung DSZ

DSZ

- Konkretisierung auf Überwachbarkeit

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

WER SIND DIE MITSPIELER BEIM COC

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Akteure und Rollen

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Verein zur Förderung von Verhaltensregeln (VfV)	• Verhaltensregeln erstellen, Genehmigung beantragen, Genehmigung aufrechterhalten • Code Owner von Trusted Data Processor
GDD & BvD	• Nutzung und Förderung des CoC • Mitglieder des VfV
DSZ	• Überwachungsstelle iSd Art. 41 DS-GVO • Mitglied des VfV
Diverse Aufsichtsbehörden	• Feedback und Verbesserungsvorschläge • Hilfreiche Anregungen

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

Trusted Data Processor: Stand

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Verhaltensregel	• Genehmigt am 31.10.2022 durch LfDI BW
Überwachungsstelle DSZ	• Akkreditiert am 10.11.2022 durch LfDI BW
Live-Betrieb	• Seit 16.11.2022

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

AN WEN RICHTET SICH DER TRUSTED DATA PROCESSOR?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Wer kann mitmachen?

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Auftragsverarbeiter
  - Leistungsangebot für deutschen Markt
  - Sitz in Deutschland
  - Verarbeitung personenbezogener Daten in Deutschland durch Auftragsverarbeiter

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

WELCHE ROLLE HAT DER DSB BEI DER EINFÜHRUNG EINES COC?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

DSB: Impulsgeber & Lotse

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Nutzen aus Sicht DSB

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Muster für DS-GVO konforme Datenschutzprozesse
- Muster einer Verpflichtung auf Vertraulichkeit
- Baseline für Einräumung von Kontrollrechten in AVV
- Argumentationshilfe gegenüber
  - Auftragsverarbeitern
  - Auftraggebern
- Erleichterung von Vertragsverhandlungen

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

WELCHEN NUTZEN HABEN AUFTRAGSVERARBEITER?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Nutzen aus Sicht Auftragsverarbeiter

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Einfachere Vertragsprüfung & Verhandlung

- Häufige Streitpunkte in AVV geregelt
- Abwehr überschießender Auftraggeberwünsche

Standardisierter Kontrollbedarf

- Ein Prüfbericht für alle Auftraggeber

Rechtssicherheit

- Bei Prozessen, AVV-Klauseln

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

WIE TIEF IST DER EINGRIFF IN DIE UNTERNEHMENSABLÄUFE?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Kein „Sahnhäubchen“

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Natur eines CoC

- Konkretisierung der DS-GVO
- Keine zusätzlichen Anforderungen erlaubt

Folge

- Anforderungen: sowie umzusetzen

Erleichterung

- „Wie“: Vorgegeben = kein Nachdenken mehr

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

WIE HOCH IST DER EINFÜHRUNGSAUFWAND FÜR TDP?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

WAS MUSS ICH MIT BESTEHENDEN AVV MACHEN?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

GIBT ES BESONDERHEITEN BEI AUSLÄNDISCHEN SUBAUFTRAGNEHMERN?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

WIRD MIR EIN VERTRAGSMUSTER VOM COC VORGESCHRIEBEN?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

WER UNTERSTÜTZT BEI DER EINFÜHRUNG DES COC?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Weitere Informationen

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Verhaltensregel.eu
  - Verhaltensregel
  - Liste selbstverpflichteter Unternehmen
  - Antragsunterlagen und online Einreichung
- Fortbildungen
  - BvD: 20.12.2022, 12.01.2023, 25.01.2023 jeweils von 10.00 Uhr bis 13.00 Uhr
  - Datakontext: 04.02.2023, 25.04.2023 jeweils von 10.00 bis 12.00 Uhr

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

Ansprechpartner

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Umsetzung im Unternehmen
  - GDD und BvD
- Antragsstellung (externer Vertrieb der DSZ)
  - vertrieb@verhaltensregel.eu
  - 030 / 754 391 597

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

WELCHEN NUTZEN HABEN AUFTRAGGEBER?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Nutzen aus Sicht 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
- Eigenkontrolle mit Vorgabe Inhalt
- Überwachung durch DSZ

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

WAS MUSS MAN SICH UNTER „STANDARDISIERUNG“ VORSTELLEN?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

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

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

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

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

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

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

Übersicht der Vorgaben beim Auftragsverarbeiter

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Angebot und Vertrag
- Unterbeauftragung
- Kontrolle von Unterauftragsverarbeitern
- Rechte betroffener Personen (Betroffenenrechte)
- Meldung potenzieller Verletzungen des Schutzes personenbezogener Daten
- Inhalt der Verpflichtung auf Vertraulichkeit
- Eigenkontrolle

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

WIE WIRD DIE UMSETZUNG DES COC KONTROLLIERT?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Vertrauen durch Überwachung

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Grundlage

- Art 40 (4) iVm 41 DS-GVO
- Nur nicht-öffentliche Stellen

DSZ

- Beschwerden → Anlassbezogene Überwachung
- Anlasslose Überwachung: zufallsbasiert, spätestens nach 7 Jahren

Aufsichtsbehörde

- Überwacht DSZ
- Unveränderte Zuständigkeit für AV

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

ERWARTEN MICH BEI EINEM VERSTOSS GEGEN DENCOC SANKTIONEN?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Nachbesserung & Sanktionen

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Transparenz

- Abläufe in Verhaltensregel dargestellt

Prinzip

- Abhilfe durch Auflagen

Ultima-Ratio

- Entzug & Meldung an Aufsichtsbehörde

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH

KANN DAS „SIEGEL“ TDP AUCH WIEDER ENTZOGEN WERDEN?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

WER UNTERBINDET DIE MISSBRÄUCHLICHE NUTZUNG DES „SIEGELS“?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

WAS KOSTET DIE SELBSTVERPFLICHTUNG?

© DSZ Datenschutz Zertifizierungsgesellschaft mbH

Kosten

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

- Antragsprüfung inkl. 1. Jahr: 4.990 € / Leistung
- Folgejahre (Aufrechterhaltung, anlasslose Prüfungen): 2.440 € / Leistung / Jahr
- Zusätzlich aufwandsabhängig: Beschwerde, anlassbezogene Prüfungen

© DSZ Datenschutz
Zertifizierungsgesellschaft mbH