Verhaltensregeln zur Fernwartung: Ein Code of Conduct vom bvitg

Christoph Isele

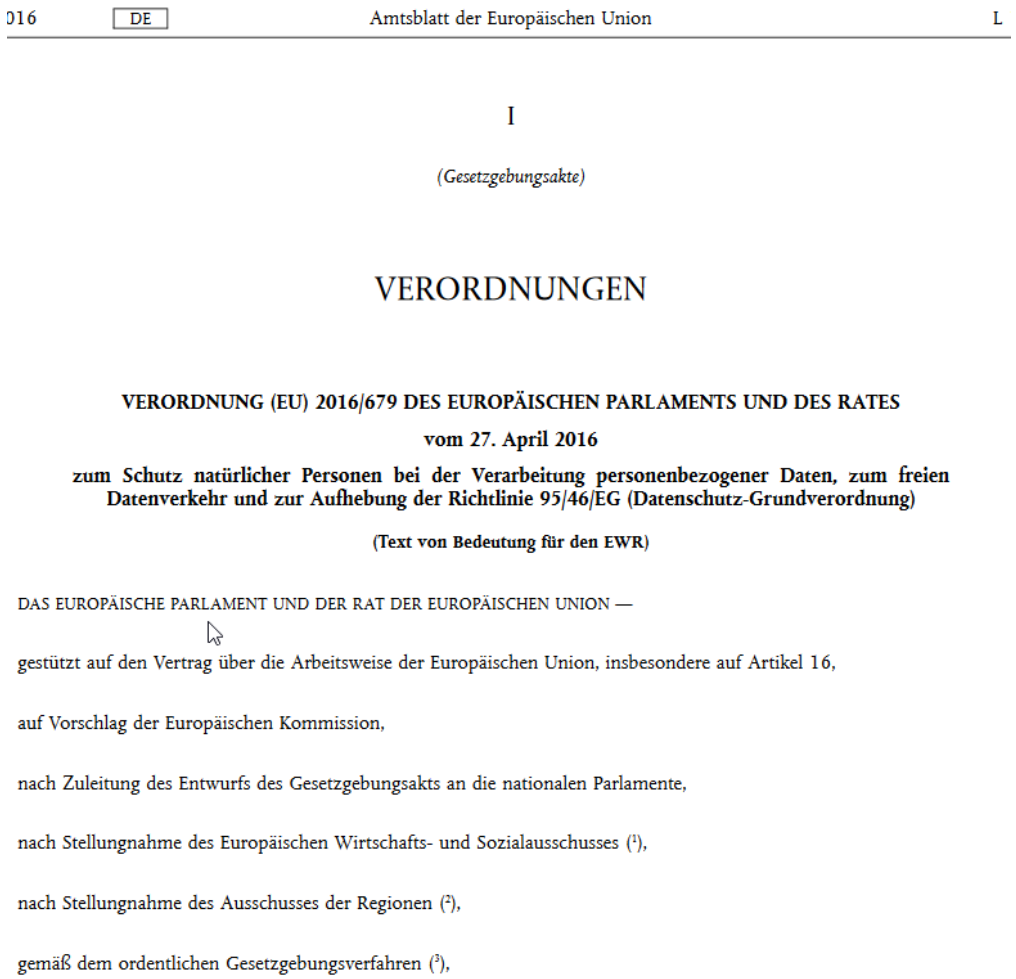
Lead Regulatory Affairs Strategist

25. Juni 2020 - Fachtagung Datenschutz im Gesundheitswesen

Agenda …

- Rechtlicher Rahmen für Verhaltensregeln
- Inhaltliche Ausgestaltung
- Aktueller Stand der Initiative

Verhaltensregeln nach Art. 40 DSGVO



016 DE Amtsblatt der Europäischen Union L

I

(Gesetzgebungsakte)

VERORDNUNGEN

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

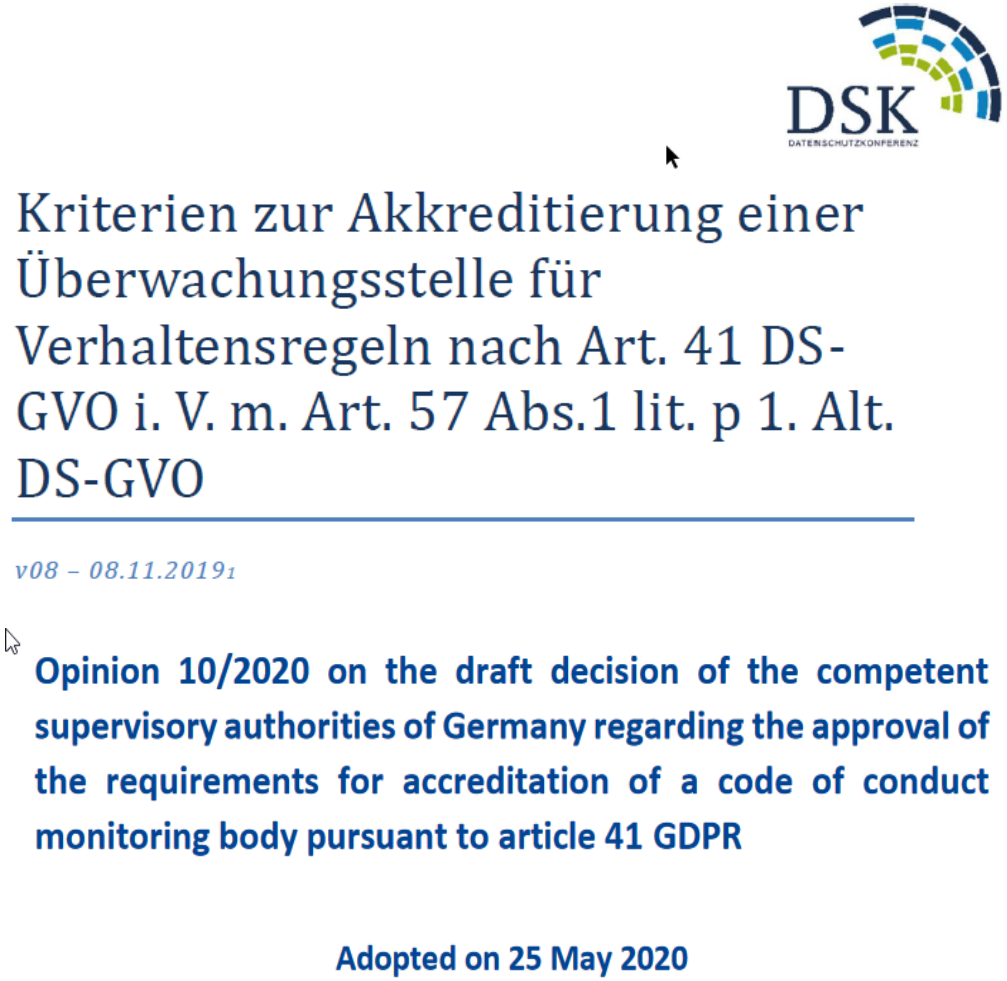
nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

nach Stellungnahme des Ausschusses der Regionen ([2]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

- Verbände … können Verhaltensregeln ausarbeiten … , mit denen die Anwendung dieser Verordnung … präzisiert wird
- Die Verhaltensregeln … müssen Verfahren vorsehen, die es der … akkreditierten Stelle ermöglichen, die obligatorische Überwachung der Einhaltung … vorzunehmen ...

Akkreditierung einer Überwachungsstelle



- Die Aufsichtsbehörde eines Mitgliedstaates stellt Kriterien für die Akkreditierung auf
- Die Kriterien wurden vom Europäischen Datenschutz Ausschuß (EDSA) geprüft,
- Danach kann die Aufsichtsbehörde eine Einrichtungen für die Überwachung akkreditieren (DAkkS unterstützt bei der fachliche Prüfung, ob die Einrichtung auditieren kann)

Aufgaben einer Überwachungsstelle

„unsere Überwachungsstelle“

- Unabhängigkeit, Fachwissen, Interessenskonflikte
- Kontrolle der zu überwachenden Unternehmen
- Führen eines Verzeichnisses
- Anlasslose stichprobenartige Überprüfung
- Beschwerdeverfahren
- Überprüfung bei Beschwerden / Dokumentation

Anforderung, Hilfestellung

- EDSA: Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679
- Vortrag BvD Herbsttagung 2018 Mirka Möldner: Verhaltensregeln (Codes of Conduct) nach Art. 40 DS-GVO

Agenda …

- Rechtlicher Rahmen für Verhaltensregeln
- Inhaltliche Ausgestaltung
- Aktueller Stand der Initiative

Verhaltensregeln·(Codes·of·Conduct)·nach·Art.·40·DS-GVO·bzgl.·„Fernwartung·in·der·Gesundheitsversorgung“¶

¶

(Verhaltensregeln·„Fernwartung·in·der·Gesundheitsversorgung“)¶

¶

Bundesverband·Gesundheits-IT·—·bvitg·e.·V.·¶

Aufgang·A,·1.·Stock
Friedrichstraße·200¶

10117·Berlin¶

¶

Verhaltensregeln „Fernwartung in der Gesundheitsversorgung“

1. Gegenstand und Ziele des Codes of Conduct
   - Einführende Beschreibung der vom CoC geregelten Verarbeitungstätigkeit(en)
   - Darstellung der Ziele des CoC
   - Begründung für die Notwendigkeit des CoC
   - Nachweis Repräsentativität des Verbandes
2. Angabe räumlicher Anwendungsbereich
   - Deutschland
3. Angabe sachlicher Anwendungsbereich
   - Sektor „Gesundheitsversorgung“
   - Kategorien von Verantwortlichen/Auftragsverarbeitern
   - Darstellung, wie der CoC die Anwendung der DS-GVO erleichtert
4. Auswahl der Aufsichtsbehörde und Kontrollstelle

Verhaltensregeln „Fernwartung in der Gesundheitsversorgung“

5. Inhaltliche Ausgestaltung

- Hauptteil (21 von 44 Seiten)
- Themen i.d.R. durch Gesetze oder Stand der Technik vorgegeben
- Daraus leiten sich die Anforderungen an die Verantwortlichen bzw. Auftrags-verarbeiter ab
- 97 Anforderungen

Verhaltensregeln „Fernwartung in der Gesundheitsversorgung“

5. Inhaltliche Ausgestaltung
    1. Vertraulichkeits-/ Geheimhaltungsvereinbarungen
    2. Vereinbarungen zur Informationsübertragung
    3. Richtlinien für die Informationsübertragung
    4. Umgang mit datenschutzrechtlichen Pflichten
    5. Umgang mit Testdaten

3 Beispiele willkürlich herausgegriffen …

Beispiel 1 – Anforderung an den Verantwortlichen

5.4 Umgang mit datenschutzrechtlichen Pflichten

5.4.1 Informationspflicht

Aus Artt. 13, 14 DS-GVO resultieren Informationspflichten, welche der Verantwortliche wahrzunehmen hat. Diese Pflichten gelten bei jeder Verarbeitung personenbezogener Daten, somit insbesondere auch bei Fernwartung.

Anforderung 39.
Werden personenbezogene Daten bei der betroffenen Person erhoben, so muss der Verantwortliche der betroffenen Person die Informationen gem. Art. 13 DS-GVO mitteilen, es sei denn, die Person verfügt bereits über die Informationen. Die Informationen müssen der betroffenen Person zum Zeitpunkt der Erhebung zur Verfügung gestellt werden.

Der Auftragsverarbeiter muss sich darauf verlassen können, dass der Verantwortliche seine Informationspflichten erfüllt hat.

Beispiel 2 – Anforderung an den Auftragsverarbeiter

5.4 Umgang mit datenschutzrechtlichen Pflichten

5.4.5 Sicherheit der Verarbeitung

Nur wenn gewährleistet ist, dass die einen Fernzugriff durchführende Person sicher identifiziert werden kann, können im Bedarfsfall Zugriffe auf sensible/kritische Daten nachvollzogen werden. Daher müssen Verantwortlicher und/oder Auftragsverarbeiter über ein Identitätsmanagementprozess verfügen, mit dem die Identitäten der Nutzer mit Zugang zu Systemen verwaltet werden.

Anforderung 48. Es existiert ein Identity Management inkl. eines zentralen Benutzermanagements, welches bei jedem Fernwartungsvorgang die Identität der zugreifenden Personen gewährleistet.

Anforderung 49. Es müssen Benutzerkonten verwendet werden, welche die eindeutige Identifizierung des Benutzers ermöglichen.

Anforderung muss vom Auftragsverarbeiter erfüllt werden

Beispiel 3 – Verantwortlicher und Auftragsverarbeiter

5.5 Umgang mit Testdaten

5.5.1 Zugangssteuerung

Ein Zugriff auf ein Produktivsystem beinhaltet immer auch das Risiko der Beeinträchtigung– ob gewollt oder ungewollt – des Produktivsystems. Daher sollte, wann immer möglich, ein Zugriff auf das Produktivsystem vermieden und stattdessen mit Testumgebungen gearbeitet werden

Anforderung 93. Die Fernwartung erfolgt, wenn möglich in Testumgebungen; der Zugriff auf das Produktivsystem sollte nur gewählt werden, wenn ein Wartungsziel anders nicht erreicht werden kann.

Anforderung 94. Die Zugangssteuerungsverfahren, die für den Einsatz der Produktivsysteme gelten, gelten auch für die Testsysteme.

Anforderung kann nur erfüllt werden wenn beide ihren Teil umsetzen.

Verhaltensregeln „Fernwartung in der Gesundheitsversorgung“

6. Bezugsrahmen zur Datenschutz-Grundverordnung
   1. Bezugsrahmen zu rechtlichen Vorgaben
   2. Abgleich mit anwendbarem europäischen Recht
   3. Abgleich mit anwendbarem nationalen Recht
      - Gesundheitsdaten: Bundes-, Landes- und Kirchenrecht –
        Heterogenität der dt. Gesetzgebung erschwert Erstellung CoC beträchtlich!
      - Beschäftigtendaten = Arbeitsrecht
      - Strafgesetzbuch: § 203 StGB
      - Berufsrecht
      - Sozialdatenschutz
   4. Auseinandersetzung mit anwendbaren Working Papers des EDSA
      - EDSA-Leitlinie 1/2019

Verhaltensregeln „Fernwartung in der Gesundheitsversorgung“

7. Verteilung der Anforderungen auf den Verantwortlichen und den Auftragsverarbeiter

54	Verantwortlicher
24	Auftragsverarbeiter
29	Verantwortlicher und Auftragsverarbeiter

Verhaltensregeln „Fernwartung in der Gesundheitsversorgung“

8.1.1 Verantwortliche

- Deutsche Krankenhausgesellschaft e.V.
- Bundesärztekammer
- Deutscher Hausärzteverband e.V.
- Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter KH-IT e. V.
- KBV - Kassenärztliche Bundesvereinigung KdöR

8.1.2 Auftragsverarbeiter

- Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
- BVMed - Bundesverband Medizintechnologie
- fbmt - Fachverband Biomedizinische Technik
- Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI)

8.1.3 Betroffene Personen

Betroffene Personen sind Beschäftigte bei den jeweiligen Verantwortlichen.

- Vereinte Dienstleistungsgewerkschaft - ver.di
- Deutsche Berufsverband für Pflegeberufe e. V. (DBfK)

8. Erfolgte Konsultation

Die Verhaltensregeln sind auch im Bereich der Apotheken anwendbar, obwohl wir keine Apothekenvertreter zur Konsultation eingeladen haben.

Verhaltensregeln „Fernwartung in der Gesundheitsversorgung“

9. Anforderungen an die Prüf-/Kontrollstelle
   - Befugnisse der Kontrollstelle
   - Beitritt zum Code
   - Kontrolle der Verhaltensregeln
   - Berichtswesen
   - Beschwerdemanagement

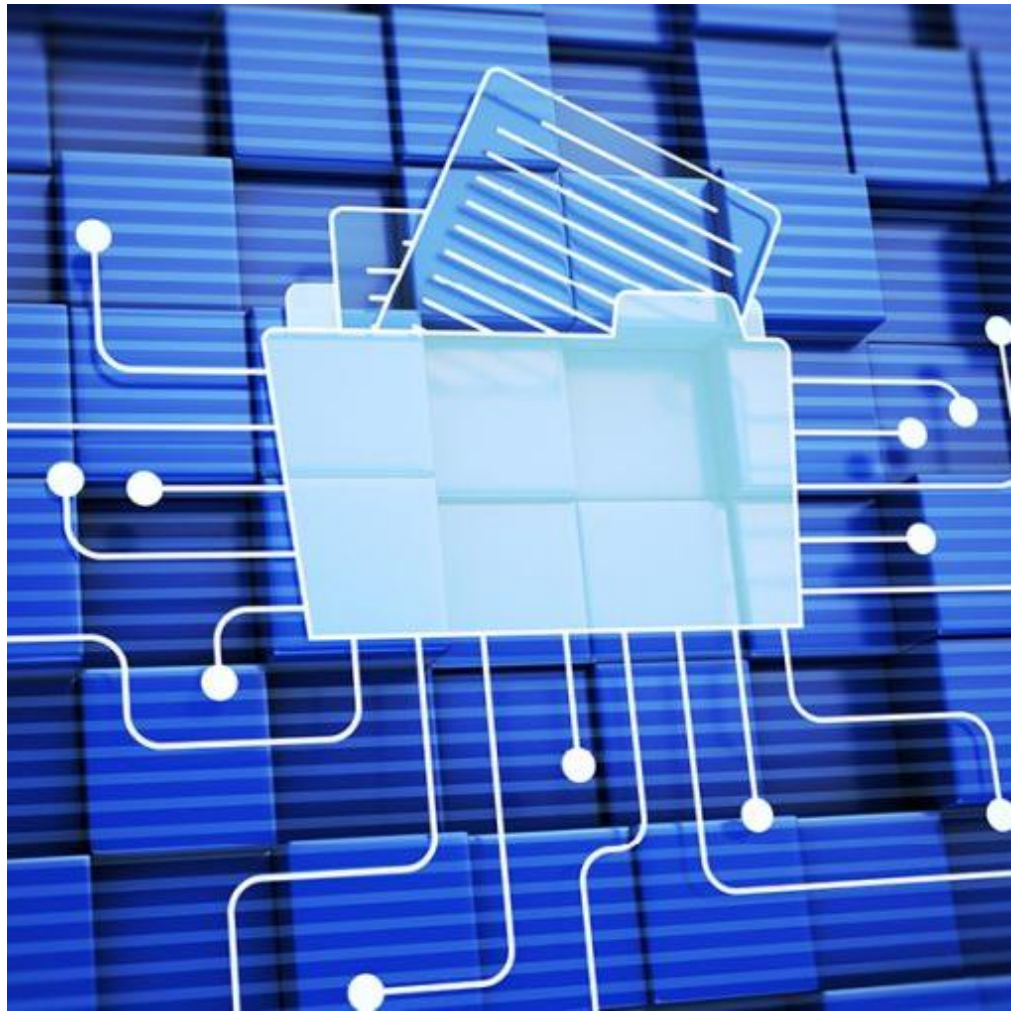
10. Überprüfung dieser Verhaltensregeln

…

(Anhänge)

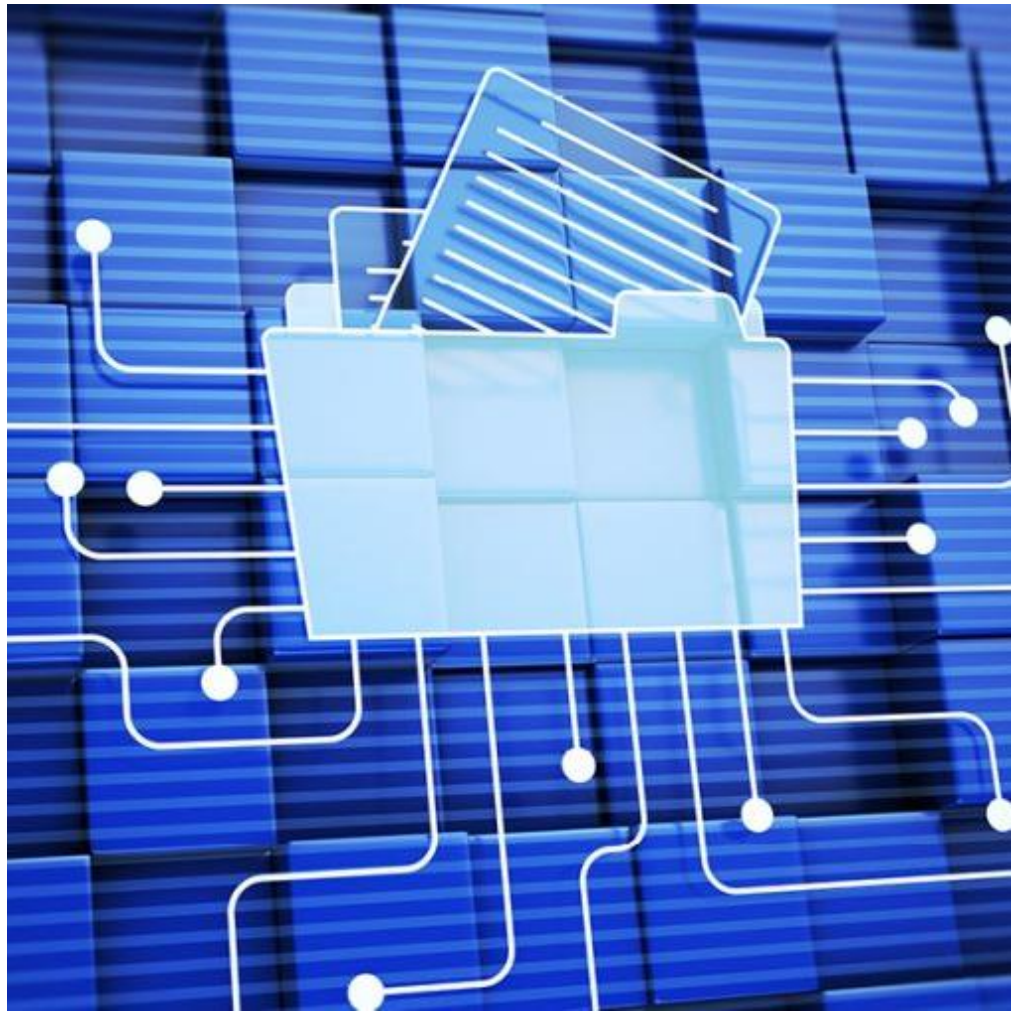
- Rechtlicher Rahmen für Verhaltensregeln
- Inhaltliche Ausgestaltung
- Aktueller Stand der Initiative

Aktueller Stand und weiteres Vorgehen



- ✓ Interne Finalisierung des CoC
- ✓ Abstimmung mit der Überwachungsstelle: CoC in vorliegender Form aus ihrer Sicht prüfbar?
- ✓ Frühe Kontaktaufnahme und Information der ausgewählten Aufsichtsbehörde
- Öffentliche Konsultation (läuft)
  - Verbände von Verantwortlichen und Auftragsverarbeitern, z.B.
    DKG, BÄK, bitkom, …
  - Verbände Beschäftigter als Betroffenenvertreter, z.B.
    ver.di, DBfK, …
  - Berücksichtigung der Rückmeldungen im CoC (geplant bis 2. Dezemberwoche)
- Einreichung des CoC bei der Aufsichtsbehörde, möglichst bis Ende diesen Jahres

Fragen?



- ✓ Gruppe mit 8 Autoren
- ✓ Sie erreichen uns über Bernd Schütze, mich oder die Geschäftsstelle des bvitg

Vielen Dank für Ihre Aufmerksamkeit

Christoph Isele

christoph.isele@cerner.com

Weitere Literatur

EDSA:

Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679

DSK:

Kriterien zur Akkreditierung einer Überwachungsstelle für Verhaltensregeln nach Art. 41 DS-GVO i.V.m. Art. 57 Abs.1 lit. p 1. Alt. DS-GVO

EDSA:

Opinion 10/2020 on the draft decision of the competent supervisory authorities of Germany regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR