Deutsche Stiftung für Recht und Informatik

Der Nachweis der Sicherheit der Verarbeitung im Rahmen datenschutzrechtlicher Zertifizierungen

Maximilian Kessemeier - Lucas Blum
Schürmann Rosenthal Dreyer Rechtsanwälte PartmbB - DLA Piper UK LLP

Herbstakademie 2021

Überblick

- Datenschutzrechtliche Zertifizierungen
  - Zertifizierungen im Sinne der DSGVO
  - Zweck von datenschutzrechtlichen Zertifizierungen
- Inhalt von Zertifizierungsprogrammen
  - Beteiligte im Rahmen der Zertifizierung
  - Struktur von Zertifizierungsprogrammen
- Die Sicherheit der Verarbeitung
  - Anforderungen und Herausforderungen
  - Abbildung in Zertifizierungsprogrammen
- Fazit

Zertifizierungen im Sinne der DSGVO

Nach Art. 42 Abs. 1 S. 1 DSGVO haben die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und –prüfzeichen zu fördern.

- Erstmals umfassende europaweite Grundlage von datenschutzspezifischen Zertifizierungsverfahren sowie Datenschutzsiegeln und –prüfzeichen
- Art. 42 DSGVO regelt die Anforderungen an die Zertifizierung gibt aber kein konkretes Zertifizierungsverfahren vor
- Art. 43 DSGVO regelt die Anforderungen an die Akkreditierung und Arbeit der Zertifizierungsstellen

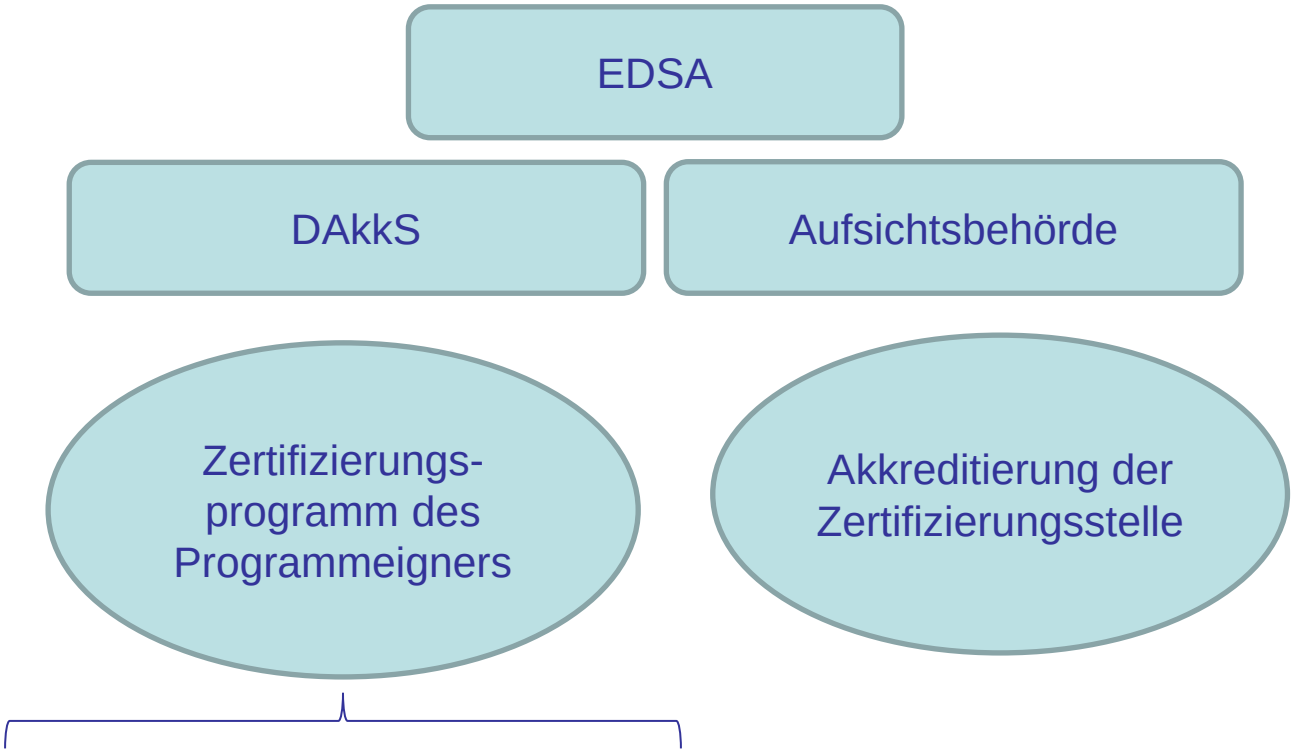
Zweck von datenschutzrechtlichen Zertifizierungen

"(…) die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.", vgl. Art. 42 Abs. 1 S. 1 DSGVO

- Verantwortliche und Auftragsverarbeiter müssen die Einhaltung der Vorgaben der DSGVO nachweisen können, vgl. etwa Art. 5 Abs. 2 DSGVO, Art. 24 Abs. 1 DSGVO (Rechenschaftspflicht/Accountability)
  - Nachweis durch Zertifizierung "als Faktor" möglich (vgl. bspw. Art. 24 Abs. 3, Art. 25 Abs. 3, Art. 28 Abs. 5 oder Art. 33 Abs. 3 DSGVO)

- Transparenz erhöhen und den betroffenen Personen einen raschen Überblick über das Datenschutzniveau ermöglichen, vgl. ErwG 100
  - Schaffung von Marktanreizen/Wettbewerbsvorteilen

Genehmigung eines Zertifizierungsprogramms



- **Konformitätsbewertungsprogramm**
  z.B. Methoden, Anforderungen an Zertifizierungsstelle
- **Kriterienkatalog**
  Anforderungen an Verarbeitungstätigkeit

Reichweite von Zertifizierungsprogrammen

Allgemeines Zertifizierungsprogramm

- *a certification scheme that targets a large range of different processing operations performed by a data controller/processor from various sectors of activity*

→ Kritik: Erhöhen nicht die Transparenz

Spezifisches Zertifizierungsprogramm

- *a certification scheme that targets specific processing operations performed by a data controller/processor (e.g.: pseudonimyzation of personal data, human resources processing) and / or for a specific sector of activity (example: data processing in stores)".*

→ Kritik: Nur für kleinen Kreis von Verarbeitungen relevant

Damit zusammenhängend Frage der Spezifität von Zertifizierungskriterien bzw. deren Skalierbarkeit → Stets zu berücksichtigen:
Zertifizierungskriterien müssen Anforderungen der DSGVO aufnehmen

Zertifizierung geeigneter technischer und organisatorischer Maßnahmen des Art. 32 DSGVO

- Relevant für eine Zertifizierung nach Art. 32 Abs. 3 DSGVO aber auch anderer Zertifizierungsverfahren, vgl. bspw. Art. 28 Abs. 3 S. 2 lit. c) DSGVO
- Zertifizierungskriterien müssen die Anforderungen der DSGVO aufnehmen:
  - Verantwortliche und Auftragsverarbeiter müssen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten

Hierbei zu berücksichtigen: Stand der Technik, Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Herausforderung bei der Bestimmung von Zertifizierungskriterien für die Zertifizierung der Sicherheit der Verarbeitung

- Angemessene Schutzniveau bestimmt sich nach der konkreten Verarbeitung → Risikobasierter Ansatz
- DSGVO gibt grundsätzlich keine bestimmten technischen und organisatorischen Maßnahmen vor
- Zu berücksichtigende Faktoren können sich ändern, z.B. Zweck der Verarbeitung, Stand der Technik

Unsere Einschätzung: Bei der Zertifizierung der Sicherheit der Verarbeitung sind Kriterien in der Form vorgegebener technischer und organisatorischer Maßnahmen in der Regel nicht geeignet

Ansatz zur Zertifizierung der Sicherheit der Verarbeitung

1. Kriterium: Beschreibung der Verarbeitung und Durchführen einer Risikobewertung

2. Kriterium: Ermittlung und Festlegen des angemessenen Schutzniveaus

3. Kriterium: geeignete TOMs identifizieren und umsetzen (SDM)

4. Kriterium: Prüfung Vorliegen angemessenes Schutzniveau

5. Kriterium: Soweit erforderlich geeignete TOMs identifizieren und umsetzen (SDM)

6. Prüfung Vorliegen angemessenes Schutzniveau

Fazit

- Datenschutzrechtliche Zertifizierungsverfahren sind zu begrüßen und erleichtern den Nachweis der Einhaltung der Anforderungen der DSGVO.
- Zertifizierungskriterien zur Konkretisierung der Anforderungen des Art. 32 DSGVO stellen eine besondere Herausforderung dar.
- Zertifizierungskriterien können geeignete TOMs oder einen Prozess zur Bestimmung geeigneter TOMs vorgeben.
- Programmeigner sowie Verantwortliche und Auftragsverarbeiter sollten den für die jeweilige Verarbeitungstätigkeit passenden Ansatz wählen.

Ihre Ansprechpartner

Maximilian Kessemeier
Rechtsanwalt
Schürmann Rosenthal Dreyer Rechtsanwälte

Mail: kessemeier@srd-rechtsanwaelte.de
Telefon: +49 (0)30 / 213 002 80

Lucas Blum
Rechtsanwalt | Associate
DLA Piper UK LLP

Mail: lucas.blum@dlapiper.com
Telefon: +49 89 23 23 72 132