

Bonn, 10. Juli 2015

Information

EU-Datenschutz-Grundverordnung setzt auf Zertifizierung der Auftragsdatenverarbeitung



Nachdem der Rat der Europäischen Union im Juni 2015 seine Position hinsichtlich einer EU-Datenschutz-Grundverordnung (EU-DS-GVO) mit dem Ziel eingenommen hat, die Verhandlungen mit Kommission und Europäischem Parlament im Rahmen des so genannten „Trilog“ bis Ende des Jahres 2015 zum Abschluss zu bringen, mehren sich die Fragen nach einer Vereinbarkeit der Zertifizierung der DSZ mit den neuen gesetzlichen Vorgaben.

Zunächst ist festzustellen, dass auch unter einem neuen gesetzlichen Regelwerk an der **Auftragsdatenverarbeitung** durch Normierung in Artikel 26 **festgehalten werden soll**. Hier zeichnet sich weiterhin die Tendenz ab, dass verantwortliche Stellen einen so genannten „Auftragsverarbeiter“ auszuwählen haben, der **hinreichende Garantien** dafür bietet, dass

- seine **technisch-organisatorischen Maßnahmen** im Einklang mit den Anforderungen der EU-DS-GVO durchgeführt werden sowie
- Rechte der Betroffenen durch **geeignete Sicherheitsvorkehrungen** geschützt werden.

Mit Blick auf konkrete Anforderungen an Auftragsverarbeiter enthält Artikel 26 **deutliche Parallelen zu § 11 BDSG**; so u.a.

- die Sicherstellung einer weisungsgemäßen Auftragsausführung
- die Ermöglichung einer Überprüfung der getroffenen und vereinbarten Maßnahmen durch den Auftraggeber
- den Nachweis der Einhaltung der gesetzlichen Vorgaben
- die Unterstützung des Auftraggebers bei der Wahrung von Rechten der Betroffenen (Information, Auskunft, Berichtigung, Löschung, Datenportabilität, Widerspruch)
- das Vorhalten unterstützender Maßnahmen bei Sicherheitsvorfällen und hierbei erforderlicher Meldepflichten gegenüber Aufsichtsbehörden und Betroffenen
- die Vereinbarung und Kontrolle technisch-organisatorischer Maßnahmen bei Subunternehmern,
- verpflichtende Maßnahmen nach Vertragsbeendigung, so die Datenlöschung.

Hinzu kommen **neue Verantwortlichkeiten** für Auftragsverarbeiter innerhalb der EU-DS-GVO, so u.a. bei

- der Implementierung technisch-organisatorischer Maßnahmen nach dem Stand der Technik auf Basis einer vorherigen Risikobewertung mit dem Auftraggeber
- der Durchführung von Datenschutz-Folgenabschätzungen nach Artikel 33
- der Konsultation von Aufsichtsbehörden.

Die Bestärkung bestehender Pflichten auf Seiten des Auftragsdatenverarbeiters sowie die Einführung neuer Obliegenheiten, machen die Einführung **standardisierter Maßnahmen, Prozesse und Kontrollen** auf Seiten des Dienstleisters im Sinne des Datenschutzstandards DS-BvD-GDD-01 damit umso notwendiger.

Die Reformbestrebungen aus Brüssel zeigen, dass der von der DSZ eingeschlagene Weg in Gestalt der Zertifizierung von Auftragsdatenverarbeitern über ein transparentes und unabhängiges Prüfverfahren der richtige ist. Nach Verabschiedung einer EU-DS-GVO wird der Datenschutzstandard als Prüfgrundlage der Zertifizierung an relevante gesetzliche Neuerungen einer EU-DS-GVO angepasst werden, so dass eine Zertifizierung auch mit einer neuen europäischen Vorgabe stattfinden wird.

DSZ Datenschutz Zertifizierungsgesellschaft mbH

Die DSZ Datenschutz Zertifizierungsgesellschaft mbH zertifiziert Unternehmen nach dem Datenschutzstandard für Auftragsdatenverarbeiter DS-BvD-GDD-01. Das Unternehmen zertifiziert ebenfalls Auditoren, die Audits nach DS-BvD-GDD-01 durchführen. Getragen wird die DSZ Datenschutz Zertifizierungsgesellschaft mbH von den Fachverbänden „Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.“ und „Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.“

Ihr DSZ-Ansprechpartner:

Geschäftsstelle Bonn, Heinrich-Böll-Ring 10, 53119 Bonn

Tel: 0228/96 96 75 22, E-Mail: info@dsz-audit.de, Internet: <http://www.dsz-audit.de>

Geschäftsstelle Berlin, Budapester Straße 31, 10787 Berlin

Tel: 030/20 62 14 42, E-Mail: info@dsz-audit.de, Internet: <http://www.dsz-audit.de>