

Auftragsdatenverarbeitung – Zertifizierung von Dienstleistern und vertragliche Feinheiten

RA Sascha Kremer, Geschäftsführer der LLR Data Security and Consulting GmbH, externer Datenschutzbeauftragter und Partner der Sozietät LLR Legerlotz Laschet Rechtsanwälte, sowie RA Andreas Jaspers, Geschäftsführer der Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD), beleuchteten am 4.12.2013 das Thema Auftragsdatenverarbeitung.

RA Kremer referierte aus juristischer Sicht. Nach Erläuterung der datenschutzrechtlichen Grundlagen, einschließlich der zentralen Norm des § 11 BDSG und der Abgrenzung zur Funktionsübertragung, skizzierte er die empfehlenswerten Bestandteile eines Vertrages über die Auftragsdatenverarbeitung, insbesondere die Regelungen zu Subunternehmern, zum Datenschutzkonzept, zu Kontrollen, Kosten und der Haftung. In Bezug auf Subunternehmer sei eine Aufzählung der Mindestvoraussetzungen sinnvoll, insbesondere hinsichtlich der Tätigkeit auf europäischem Gebiet sowie der Fachkunde und Liquidität. Für den Fall von Vertragsverstößen fehle zudem oft eine Widerrufsregelung. Ein Problempunkt beim Datenschutzkonzept sei die Regelung des Verfahrens bei der Aktualisierung der Vereinbarung über technisch-organisatorische Maßnahmen nach der Anlage zu § 9 BDSG. Auch einer schleichenden Absenkung des ursprünglich vereinbarten Datenschutzniveaus sei vorzubeugen. Im Rahmen von Kontrollen seien Mitwirkungspflichten des Auftragnehmers zu vereinbaren. Kosten von Audits und Auskünften seien vertraglich zu verteilen, andernfalls diese Punkte zu einer Kostenfalle führen könnten. Vertragsstrafen im Rahmen der Haftung bei Datenschutzverstößen seien schließlich ein gangbarer Weg, um herauszufinden wie ernst es der Auftragnehmer mit dem Datenschutz meine.

Im Rahmen der Diskussion wurde das Problem angesprochen, dass viele Auftraggeber bei der Auswahl des Vertragspartners strikt nach dem Preis der Grundleistung gingen und in die Falle bezüglich der Folgekosten tappten. Außerdem behandelte man die Frage nach der praktischen Relevanz von Bußgeldern: diese seien momentan noch die Ausnahme, während Beanstandungen in Prüfberichten der Aufsichtsbehörden schon häufiger anzutreffen seien.

Der praxisorientierte Beitrag von RA Jaspers trug der Tatsache Rechnung, dass es sich häufig als schwierig erweist, einen qualifizierten Auftragsdatenverarbeiter auszuwählen. Um die Qualität der Auftragsverarbeiter vergleichbarer zu gestalten, entwickelte die Gesellschaft für Datenschutz und Datensicherheit in Zusammenarbeit mit dem Berufsverband der Datenschutzbeauftragten Deutschlands den Datenschutzstandard „DS-BvD-GDD-01“, dessen Datenschutzsiegel im Wege einer Zertifizierung erworben werden kann. RA Jaspers erläuterte die Reichweite des Standards und die inhaltlichen Voraussetzungen der Zertifizierung sowie den Nutzen für die Beteiligten. Während herkömmliche Zertifikate und Gütesiegel häufig die Schwäche aufwiesen, dass deren Kriterien, Zertifizierungsgegenstand und Prüfberichte geheim seien und das Zertifizierungsverfahren einstufig gestaltet, die Zertifizierungsstelle also zugleich der Auditor sei, sei der DS-BvD-GDD-01 ein offener Standard mit hoher Transparenz. Die Prüfung erfolge zudem ausschließlich durch ausgebildete Auditoren und die Gesamtkonzeption werde auch vom Landesdatenschutzbeauftragten Nordrhein-Westfalen befürwortet.

Die Diskussionsrunde hatte die angehende EU-Datenschutzgrundverordnung zum Gegenstand. Auch diese kenne die Auftragsdatenverarbeitung und setze zudem stark auf Zertifizierung. Obwohl diesbezügliche Vorgaben aus Brüssel mit Sicherheit kommen würden, sei es nicht sinnvoll, sie erst abzuwarten, da die Verordnung im Rahmen der laufenden Legislaturperiode nicht zu erwarten sei. Außerdem wurden die Kosten der Zertifizierung, einschließlich derjenigen der Vorbereitung, der Prüfung durch den Auditor und der Siegelerteilung benannt: insgesamt 20.000-25.000€