ausländische Cloud-Anbieter verarbeiten zu lassen. Die Zulässigkeit richtet sich nach den §§ 4 b und 4 c und § 28 Abs. 1 Satz 1 Nr. 2.

2a.9 Cloud Computing ist ein Angebot, das technisch möglich ist und ökonomisch sinnvoll sein kann. Allerdings wurden bei der Entwicklung dieser Technologie verfassungsrechtliche und vor allem datenschutzrechtliche Gesichtspunkte vernachlässigt. Es ist daher dringend notwendig, einen **europäischen Rechtsrahmen** zu schaffen, der es ermöglicht, Cloud Computing unter Berücksichtigung des Datenschutzes und der Datensicherheit als Möglichkeit des Outsourcing einzusetzen. Vgl. dazu die Stellungnahme der Art. 29-Datenschutzgruppe vom 1. 7. 2012 (Opinion 05/2012 on Cloud Computing, WP 196, unter www.ec.europa.eu/justice/data-protection/article-29/index_de.htm). **15g**

2a.10 Eine **Orientierungshilfe** zum Thema Cloud Computing des Arbeitskreises Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. 9. 2011 setzt sich mit der Frage des **datenschutzrechtlichen Einsatzes** dieser Technologie auseinander. Die Orientierungshilfe richtet sich an Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche (www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf). **15h**

Checkliste beim Einsatz von Cloud Computing **15i**

I. Auswahl des Cloud-Anbieters

1. Schutzbedarfsanalyse hinsichtlich
   - Vertraulichkeit
   - Integrität
   - Verfügbarkeit
   - Revisionssicherheit

1.1 Dokumentation der Analyse

1.2 Prüfung, ob die Sicherheitsanforderungen erfüllt werden

1.3 Feststellung des Restrisikos

1.4 Bewertung des Restrisikos und dessen Akzeptanz

2. Nachweis einer sicheren und ständig verfügbaren Netzwerkkommunikation
3. Nachweis eines IT-Sicherheitskonzeptes (Information Security Management Systems ISM) nach ISO 27001 auf der Basis von IT-Grundschutz oder ISO 2700 x
4. Nachweis eines Sicherheitszertifikats über das Sicherheitskonzept

II. Vertragliche Regelungen

1. Benennung aller Unter-Anbieter, sämtlicher möglichen Verarbeitungsorte (z. B. innerhalb oder außerhalb der EU) und der jeweiligen Inhalte nach Abs. 2 Nr. 6
2. Regelung der Verantwortlichkeiten und Ansprechpartner des Cloud-Anbieters
3. Regelung eines vertragsstrafenbewehrten Weisungsrechts zur Realisierung der Betroffenenrechte (z. B. Berichtigung, Sperrung, Löschung, Auskunft)
4. Festlegung der Vertragssprache und des Gerichtsstandes
5. Festlegung regelmäßiger Sicherheitsprüfungen durch Cloud-Anbieter oder externem Dienstleister über die Realisierung der technischen und organisatorischen Datensicherungsmaßnahmen nach § 9, insbes. Zugriffskontrolle, Verschlüsselung, Löschung.