Friederike Voskamp, Dennis-Kenji Kipker, Richard Yamato

Grenzüberschreitende Datenschutzregulierung im Pazifik-Raum

Das Cross Border Privacy Rules-System der APEC – ein Vergleich mit den Binding Corporate Rules der EU

Im Juli 2012 traten die USA als erster Staat dem Cross Border Privacy Rules-System der Asia-Pacific Economic Cooperation (APEC) bei. Die Teilnahme an diesem freiwilligen System grenzüberschreitender Datenschutzregulierung läutete damit ein neues Stadium im internationalen Datenschutz im Pazifikraum ein. Vorliegender Beitrag stellt Entstehung, Teilnahmevoraussetzungen und Wirkungsweisen des Systems dar und vergleicht dieses mit den europäischen Binding Corporate Rules.

1 Einleitung

Am 26. Juli 2012 gab die US-Wirtschaftsministerin Blank die Teilnahme der Vereinigten Staaten von Amerika an dem *Cross Border Privacy Rules* (CBPR)-System der *Asia-Pacific Economic Cooperation* (APEC) bekannt. Mit dieser Teilnahme sind die USA insofern Vorreiter, als sie der erste Staat waren, der sich für die aktive Partizipation an diesem Projekt entschieden hat. Blank bezeichnete den Beitritt auch deshalb als „wichtigen Meilenstein des internationalen Datenschutzes".[1] Kaum sechs Monate später folgte Mexiko und trat dem CBPR-System ebenfalls bei[2] und eröffnete somit erstmals die Perspektive einer tatsächlichen Umsetzung des Systems im grenzüberschreitenden Datenverkehr.

Bevor die einzelnen Aspekte des CBPR-Systems beleuchtet werden, wird im Folgenden zunächst dargestellt, aus welchen rechtlichen Strukturen und wirtschaftspolitischen Ideen dieses System hervorgegangen ist:

Friederike Voskamp

Wissenschaftliche Mitarbeiterin und Doktorandin am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen

E-Mail: voskamp@uni-bremen.de

Dennis-Kenji Kipker

Wissenschaftlicher Mitarbeiter und Doktorand am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen

E-Mail: kipker@uni-bremen.de

Richard Yamato

Wiss. Mitarbeiter am Lehrstuhl für Rechtsphilosophie und Öffentliches Recht (Prof. Dr. Volkmann) und Doktorand am völker- und medienrechtlichen Lehrstuhl von Prof. Dr. Dörr, JGU Mainz
E-Mail: ryamato@uni-mainz.de

2 Das APEC Privacy System

Die APEC ist ein 1989 in Canberra ins Leben gerufenes internationales Forum wirtschaftlicher Zusammenarbeit im pazifischen Raum,[3] das zunächst als informales Dialogforum auf Minister-Ebene tagte; seit 1993 treffen sich die Regierungs- und Staatschefs der mittlerweile 21 Mitgliedstaaten[4] jährlich im Rahmen des *APEC Economic Leaders' Meeting*, um im Rahmen multilateraler Zusam-

1 Presseerklärung des US-Wirtschaftsministeriums v. 26.7.2012, abrufbar unter: http://www.commerce.gov/news/press-releases/2012/07/26/acting-us-commerce-secretary-rebecca-blank-announces-us-participation (Stand aller Verlinkungen jeweils der 10.4.2013).

2 Presseerklärung der APEC v. 16.1.2013, abrufbar unter: http://www.apec.org/Press/News-Releases/2013/0116_cbpr.aspx.

3 Vgl. General Principles of APEC: Chairman's Summary Statement of the APEC Ministerial Meeting 1989, Rn. 17 – zusammen mit den Erklärungen der Ministerial Meetings in Singapur 1990 und Seoul 1991 auch "basic principles of APEC" genannt; dieses und alle folgenden zitierten Meeting Papers sind abrufbar unter: http://www.apec.org – sonstige zitierte APEC-Dokumente sind abrufbar unter: http://mddb.apec.org.

4 Die APEC selbst spricht von „Member Economies" und nicht von „Member States", so dass auch Hongkong und Taiwan eigenständige APEC-Mitglieder sind.

menarbeit wirtschaftliches Wachstum in der Pazifikregion zu fördern. Im Laufe der Zeit entwickelten sich weitere Themenschwerpunkte ohne unmittelbaren wirtschaftspolitischen Bezug, wie z.B. die Bekämpfung des internationalen Terrorismus.[5] Zu den Mitgliedern gehören heute insbesondere die USA, China, Russland, Japan und Australien sowie weitere pazifische sowie südamerikanische Staaten; die Summe der Bruttoinlandsprodukte der Mitgliedstaaten umfasst dabei mehr als 54% des weltweiten Bruttoinlandsprodukts.[6] Untypisch für eine internationale Wirtschaftsorganisation ist hierbei, dass die APEC bisher ausschließlich auf rechtlich unverbindlichen Absprachen beruht und kein institutionalisierter Verhandlungsmechanismus existiert;[7] Entscheidungen jeglicher Art werden daher nur im Konsens getroffen. Als intergouvernementales wirtschaftspolitisches Forum hängen Zielsetzungen, Maßnahmen, Umfang und Erfolg der Kooperation somit von der Bereitschaft der einzelnen Mitgliedstaaten ab, inwieweit sie sich engagieren und für die Ziele einsetzen.

2.1 APEC Privacy Framework

Mit dem Datenschutz befasste sich die APEC zum ersten Mal umfassend im Jahr 2004, als sie im Rahmen des *16th APEC Ministerial Meeting* in Santiago (Chile) das *APEC Privacy Framework* beschloss, das im Folgejahr noch weiter ergänzt wurde und langfristig die Etablierung eines Systems grenzüberschreitender Datenschutzregeln für Unternehmen, so genannter *Cross Border Privacy Rules* (CBPR), anvisierte.[8] Maßgeblicher Gesichtspunkt bei den Verhandlungen war die Notwendigkeit, im Zeitalter des E-Commerce einheitliche Ansätze für einen flexiblen Datenschutz im Pazifik-Raum zu verfolgen; gleichzeitig sollen keine unnötigen Hürden für den grenzüberschreitenden Informationsfluss aufgestellt werden.[9]

Die Erklärung beinhaltet außerdem neun Datenschutz-Prinzipien (part iii. *APEC information privacy principles*):

- *Preventing Harm* (Schutz vor Datenmissbrauch)
- *Notice* (Hinweispflicht der Dienstanbieter)
- *Collection Limitation* (Datensparsamkeit)
- *Uses of Personal Information* (Zweckbindungsgrundsatz)
- *Choice* (Wahlmöglichkeit der Betroffenen über Datenerhebung und -verarbeitung)
- *Integrity of Personal Information* (Richtigkeit und regelmäßige Aktualisierung der Daten)
- *Security Safeguards* (Datensicherheit)
- *Access und Correction* (Rechte der Betroffenen über Datenerhebung und -verarbeitung zu erfahren und Daten zu korrigieren)
- *Accountability* (Verantwortlichkeit des Datenverarbeiters).

Des Weiteren enthält die Erklärung Leitlinien für die Umsetzung (part iv. *implementation*) und eine Kommentierung der neun Prinzipien, die einerseits (insbesondere für den E-Commerce) ein einheitliches Datenschutzniveau garantieren, andererseits aber auch den freien Datenaustausch innerhalb der APEC nicht beeinträchtigen sollen.

2.2 Privacy Pathfinder und CPEA

Um die Umsetzung des *APEC Privacy Frameworks* voranzutreiben, wurde 2007 in Sydney der *Privacy Pathfinder* angenommen:[10] Die Mehrheit der Mitgliedstaaten einigte sich hierbei darauf,[11] in Gestalt einzelner Projekte gemeinsam an konzeptionellen Umsetzungsrahmen zu arbeiten, um das Vertrauen der Verbraucher in den Datenschutz im Bereich des grenzüberschreitenden Informationsflusses zu stärken.

Ein Beispiel hierfür ist der Entwurf eines Mechanismus zur Zusammenarbeit bei Datenschutz-Beschwerden, die mehrere Rechtsordnungen tangieren.[12] Entsprechend ist aus der *Privacy Pathfinder*-Initiative das *Cross Border Privacy Enforcement Arrangement* (CPEA) hervorgegangen, das seit Juli 2010 Anwendung findet.[13] Der dort vorgesehene Mechanismus ermöglicht die freiwillige Teilnahme von *Privacy Enforcement Authorities* der Mitgliedstaaten, um die grenzüberschreitende Zusammenarbeit zu vertiefen und das Vertrauen der Verbraucher zu stärken. *Privacy Enforcement Authorities* sind öffentliche Stellen, die für die Durchsetzung des Datenschutzrechts zuständig sind und zumindest entsprechende formale Prüfverfahren bei möglichen Datenschutzverstößen einleiten können. Den teilnehmenden *Privacy Enforcement Authorities* wird durch das CPEA erleichtert, sich untereinander zu kontaktieren und im Rahmen von grenzüberschreitenden Prüfverfahren um „Amtshilfe" zu bitten; in geeigneten Fällen kann das Verfahren auch gänzlich an eine andere *Privacy Enforcement Authority* abgegeben werden. Jegliche Unterstützung bleibt jedoch im Ermessen der *Privacy Enforcement Authority*. Durch das CPEA wurde somit ein rechtlicher Rahmen für die freiwillige Kooperation dieser öffentlichen Stellen in den APEC-Staaten geschaffen, der im Einzelnen nicht bindend ist, jedoch einen entscheidenden, fördernden Einfluss auf den behördlichen Informationsaustausch bei Datenschutzverstößen hat und einen wichtigen Baustein für die Etablierung des CBPR-Systems bildet.

3 Das CBPR-System

Auf der Entwicklung eines solchen Systems lag nämlich der Fokus bei der Umsetzung des *APEC Privacy Frameworks*, um durch die projektgebundene Zusammenarbeit der Mitgliedstaaten – unter Berücksichtigung ihres unterschiedlichen nationalen Datenschutzniveaus – die notwendigen Attribute eines praxistauglichen Systems für Datenschutzregeln grenzüberschreitenden Informationsverkehrs herauszuarbeiten. Während das CBPR-System wie bereits erwähnt auf dem oben dargestellten *APEC Privacy Framework* basiert, wurde es in seiner jetzigen Form 2007 in Honolulu beschlossen: Es handelt sich dabei anders als beim *APEC Privacy Framework* nicht um eine rechtlich

5 Statement on Counter-Terrorism, APEC Leaders' Declaration 2001 in Shanghai.

6 Vgl. Statistische Datenbank der Weltbank, abrufbar unter: http://data.worldbank.org/country.

7 Vgl. Schöbener/Herbst/Perkams, Internationales Wirtschaftsrecht, 2010, Kap. 2, Rn. 145.

8 APEC Privacy Framework, 2004/AMM/014rev1 v. 18.11.2004, S. 36.

9 Vgl. Vorwort zur vom APEC-Sekretariat veröffentlichten Version des APEC Privacy Framework, 2005.

10 APEC Data Privacy Pathfinder, 2007/CSOM/019, angenommen durch das Joint Statement des APEC Ministerial Meeting v. 6.9.2007.

11 Die Teilnahme ist insoweit freiwillig; das Projekt kann jedoch auf Grund des Konsensus-Verfahrens natürlich nicht gegen ein Veto eines Mitgliedstaates durchgeführt werden. Die Liste der teilnehmenden 13 Mitgliedstaaten ist dem Privacy Pathfinder angehängt (Fn. 10).

12 Eine Auflistung der Projekte (Stand 2009) ist zu finden in: APEC Data Privacy Pathfinder Projects, Implementation Work Plan – Revised v. 23.2.2009, 2009/SOM1/ECSG/SEM/027.

13 Angenommen auf dem Ministerial Meeting 2009 in Singapur. Der Volltext des CPEA ist abrufbar unter: http://aimp.apec.org/Documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf.

unverbindliche Absprache aller APEC-Staaten; die CBPR werden vielmehr von den hieran teilnehmenden – in der Regel international tätigen – Unternehmen auf freiwilliger Basis selbst, beruhend auf den zuvor dargestellten neun *APEC Privacy Principles*, entworfen. Es handelt sich folglich um durch Private selbst gesetzte Datenverarbeitungsmaßstäbe, deren Qualität, Voraussetzungen und Kontrolle sich jedoch an externen Normen orientieren. Durch die CBPR in Verbindung mit den *APEC Privacy Principles* können somit private Organisationseinheiten zur Entwicklung ihrer eigenen grenzüberschreitenden Datenschutzregelungen animiert werden. Zwecksetzung des CBPR-Systems ist neben der Erleichterung dieses grenzüberschreitenden Datenverkehrs in erster Linie auch der Schutz von Kundendaten bei der Verarbeitung durch ausländische Unternehmen. Das CBPR-System soll nicht die inländischen Datenschutznormen verdrängen oder verändern, sondern vielmehr unabhängig neben diese treten. In Staaten, in denen kein Datenschutzrecht vorhanden ist, soll das CBPR-System für die Datenverarbeitung beigetretener Unternehmen ein Minimum an Betroffenenschutz generieren.[14] Wenn hingegen bereits inländische datenschutzrechtliche Verpflichtungen für Unternehmen – unabhängig von einem Beitritt zum CBPR-System – gegeben sind, bleiben diese unverändert. Dies gilt auch, wenn vorhandene nationale Datenschutzvorschriften über die Anforderungen des CBPR-Systems hinausgehen.[15] In jedem Falle jedoch hat ein teilnehmendes Unternehmen durch die CBPR vermittelte strengere datenschutzrechtliche Regelungsinstrumentarien auszuführen, selbst wenn diese die Anforderungen des nationalen Rechts übersteigen sollten. Der Beitritt in das System mag zwar freiwillig sein; sobald dieser jedoch erfolgt ist, sind die Ausführung und Beachtung der Datenschutzregelungen verbindlich.

3.1 Voraussetzungen zur Teilnahme am CBPR-System

Die Teilnahme eines Unternehmens am CBPR-System setzt stets zunächst einmal die vorherige Teilnahme des dazugehörigen Staates voraus.

a) Beitritt des jeweiligen Staates

Der Aufnahmeprozess in das CBPR-System für einzelne Staaten beginnt mit einem schriftlichen Antrag durch Stellvertreter der Regierung des jeweiligen Staates beim Vorsitz der *Electronic Commerce Steering Group* (ECSG), dem Vorsitz der *Data Privacy Subgroup* (DPS) sowie dem Vorsitz des *Joint Oversight Panel* (JOP).

Zum Zeitpunkt des Antrages muss sichergestellt sein, dass zumindest eine Datenschutzbehörde des Staates Teilnehmerin des *APEC Cross Border Privacy Enforcement Arrangement* (CPEA) ist (dazu s.o. 2.2). Eine weitere Voraussetzung zur Teilnahme am CBPR-System ist, dass der APEC-Staat anzeigt, dass er zumindest einen *Accountability Agent* einsetzen wird. Bei den *Accountability Agents* handelt es sich um von der APEC für die Dauer von einem Jahr anerkannte Organe des öffentlichen Rechts oder um unabhängige Dritte, welche die Einhaltung der vom jeweiligen Unternehmen selbst gesetzten, an die *APEC Privacy Principles* geknüpften Regelungen zur Datenverarbeitung überwachen und daneben auch für das Aufnahmeverfahren eines Antragstellers in das System zuständig sind.[16] Weitergehend muss für die Aufnahme eines Staates in das CBPR-System dargelegt werden, wie der Staat das Programm des CBPR-Systems um- und durchzusetzen beabsichtigt; hierzu müssen auch die einschlägigen nationalen Vorschriften angegeben werden. Letzte Voraussetzung für die Teilnahme am CBPR-System ist, dass das JOP dem Vorsitz der ECSG einen Bericht übermittelt, welcher bestätigt, auf welche Weise die zuvor genannten Bedingungen erfüllt wurden. Sobald der Vorsitz der ECSG dem antragenden Staat daraufhin anzeigt, dass sämtliche Voraussetzungen vorliegen, gilt ein APEC-Mitgliedstaat auch als ein Mitglied des CBPR-Systems.[17]

b) Teilnahme des einzelnen Unternehmens

Die Teilnahme von Unternehmen am CBPR-System ist freiwillig, jedoch für die teilnehmende Organisation an einen Katalog von Voraussetzungen geknüpft, der zu erfüllen ist: So muss das betreffende Unternehmen zur Aufnahme in das CBPR-System zunächst die Konformität seiner datenschutzrechtlichen Regelungsprinzipien mit denen des *APEC Privacy Framework* nachweisen. Hierzu ist u.a. eine Selbstbewertung mit einem 23-seitigen Aufnahmefragebogen[18], dem so genannten *Intake Questionnaire*, durchzuführen. Der Fragebogen enthält Fragen zum Unternehmen und zu Kontaktpersonen, zur Art der zu zertifizierenden Daten sowie zum Ort der Datenerhebung und -übertragung. Weitergehend beschäftigen sich die Fragen mit der Transparenz der Datenverarbeitung, Betroffenenrechten (u.a. Informationspflichten, der Richtigstellung/Korrektur falsch gespeicherter Datenbestände), der Sicherstellung einer Begrenzung der Datenerhebung, der Zweckbindung und Verhältnismäßigkeit der Datenerhebung, der Verantwortlichkeit, der Einwilligung in die Datenverarbeitung, der Richtigkeit und Vollständigkeit der gespeicherten Daten sowie deren Aktualität in Bezug auf die damit verfolgten Verarbeitungszwecke und der Sicherung der Daten vor Verlust und unbefugtem Zugriff.

Bei einer positiven Auswertung der Ergebnisse des *Intake Questionnaires* erfolgt die CBPR-Zertifizierung durch den jeweiligen *Accountability Agent*. Das Unternehmen, welches nunmehr CBPR-zertifiziert ist, wird auf einer von der APEC zur Verfügung gestellten Internetseite gelistet, sodass sich Verbraucher und andere Interessengruppen über die CBPR-Mitgliedschaft des Unternehmens informieren können.

3.3 Kontrolle und Durchsetzung der CBPR-Regelungen

Der Beitritt zum CBPR-System ist freiwillig. Sobald ein Unternehmen aber seine Mitgliedschaft erworben hat, sind die Datenschutzstandards der CBPR verbindlich. Um die Umsetzung und Einhaltung der CBPR sicherzustellen, veröffentlichen die APEC-Mitgliedstaaten eine allgemein zugängliche Liste aller Unternehmen, die CBPR-zertifiziert wurden. Bestandteil dieses Verzeichnisses ist auch eine sog. *contact point*-Information mit den Daten des zuständigen Ansprechpartners des Unternehmens und einer Kontaktinformation des *Accountability Agents*, welcher das Unternehmen zertifiziert hat, sowie der zuständigen Datenschutzbehörde. Auf diese Weise können betroffene Kunden sich bei Fragen und Be-

14 CBPR – Policies, Rules, Guidelines, par. 43.

15 Vgl. hierzu die Kritik von Graham Greenleaf, Five years of the APEC Privacy Framework: Failure or promise?, Computer Law & Security Report, Vol. 25, S. 29 ff., auch abrufbar unter: http://ssrn.com/abstract=2022907.

16 Zum Ernennungsverfahren von Accountability Agents vgl. CBPR – Policies, Rules, Guidelines, par.30 ff.

17 CHARTER OF THE APEC CBPR-SYSTEM JOINT OVERSIGHT PANEL, Annex A, par. 2.2 in: CBPR – Policies, Rules, Guidelines; PROTOCOLS OF THE APEC CROSS-BORDER PRIVACY RULES SYSTEM JOINT OVERSIGHT PANEL, par.1 ff.

18 APEC CBPR-SYSTEM INTAKE QUESTIONNAIRE.

schwerden über Datenschutzverstöße mit den einschlägigen Stellen in Verbindung setzen und ggf. auch den für sie zuständigen *Accountability Agent* als erste Anlaufstelle kontaktieren, falls es zu keiner Abhilfe durch das Unternehmen kommen sollte.

Die genaue Ausgestaltung der Durchsetzung der CBPR ist dagegen den Mitgliedstaaten überlassen. Die Einhaltung des CBPR-Systems für ein zertifiziertes Unternehmen soll jedenfalls durch die *Accountability Agents* und die jeweiligen staatlichen Datenschutzbehörden, die Privacy Enforcement Agencies, erzwingbar sein. Für die Vereinigten Staaten ist die FTC (*Federal Trade Commission*), für Mexiko das *Federal Institute for Access to Information and Data Protection* (IFAI) die zuständige Privacy Enforcement Agency. Die Enforcement Agencies sollen im Rahmen des CPEA bei der Durchsetzung der CBPR miteinander kooperieren. In Bezug auf die *Accountability Agents* soll diese Durchsetzbarkeit entweder mittels gesetzlicher Vorschriften oder aber durch einen privatrechtlichen Vertrag vorgesehen werden, der mit den Unternehmen geschlossen wird.

4 Vergleich des CBPR-Systems mit dem System der „Binding Corporate Rules"

Eine Selbstverpflichtung der Unternehmen im Rahmen der internationalen Datenübermittlung, wie sie die CBPR vorsehen, ähnelt in vielen Punkten dem System der verbindlichen Unternehmensrichtlinien, der so genannten *Binding Corporate Rules* (BCR), wie sie das deutsche Datenschutzrecht in Umsetzung der europäischen Vorgaben vorsieht.

4.1 Grundlagen und Abgrenzung

Das BDSG unterscheidet in Umsetzung des Art. 25 Abs. 1 EU-Datenschutzrichtlinie (DSRL 95/46/EG) zwischen Datenübermittlungen in andere EU-Mitgliedstaaten und Datenübermittlungen in Drittstaaten, §§ 4b, 4c BDSG. Während an eine Datenübermittlung in einen anderen Mitgliedstaat aufgrund des einheitlichen europäischen Datenschutzrahmens keine weitergehenden Anforderungen gestellt werden als an eine innerstaatliche Datenübermittlung, ist nach § 4b Abs. 2 BDSG eine Datenübermittlung in einen Drittstaat grundsätzlich nur zulässig, wenn ein angemessenes Datenschutzniveau in dem betreffenden Drittstaat besteht oder einer der in § 4c Abs. 1 BDSG genannten Fälle einschlägig ist.

Eine Datenübermittlung ist darüber hinaus aber nach § 4c Abs. 2 BDSG auch dann zulässig, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist. Nach § 4c Abs. 2 BDSG können sich diese Garantien unter anderem aus *Binding Corporate Rules* (BCR) ergeben. Wird ein angemessenes Schutzniveau nicht festgestellt, kann somit nach § 4c Abs. 2 BDSG eine Datenübermittlung dennoch zulässig sein, soweit diese von der zuständigen Stelle aufgrund ausreichender Garantien in Form verbindlicher Unternehmensrichtlinien genehmigt wird.[19]

Ein Unterschied besteht in der Notwendigkeit und damit auch in der Zielsetzung von BCR und CBPR: Sowohl nach dem *APEC Privacy Framework*[20] als auch nach dem nationalen Recht vieler APEC-Mitgliedstaaten ist anders als nach europäischem Recht eine Datenübermittlung ohne weitere Voraussetzungen sowohl innerhalb der CBPR-Staaten als auch in andere Staaten auch ohne zertifizierte CBPR zulässig. CBPR sind somit nicht Voraussetzung für die Zulässigkeit von Datentransfers ins Ausland, während BCR unter den genannten Umständen für die Zulässigkeit eines grenzüberschreitenden Datentransfers entscheidend sein können. CBPR kommt folglich in größerem Maße als BCR die Funktion zu, den Unternehmen die Abgleichung der eigenen Datenschutzbestimmungen hinsichtlich Datentransfers mit den Vorgaben des APEC Privacy Frameworks zu ermöglichen und ihnen den wettbewerblichen Vorteil der Zertifizierung zu gewähren.

CBPR weisen insofern eine gewisse Nähe zu *codes of conduct* auf, die das BDSG in Umsetzung des Art. 27 DSRL 95/46/EG in § 38a vorsieht. Nach § 38a BDSG können Vereinigungen Verhaltensregel-Entwürfe, so genannte *codes of conduct*, der zuständigen Behörde vorlegen, die wiederum prüft, ob diese dem geltenden Datenschutzrecht entsprechen. Damit erhalten die Verbände und Vereinigungen die Möglichkeit, eine Art Gütesiegel für ihr Datenschutzkonzept zu erhalten.[21] Ihnen wird mithin ähnlich wie bei CBPR bescheinigt, dass sie mit ihrer Interpretation des Datenschutzrechts gesetzeskonform sind.

Insgesamt bestehen dennoch mehr Gemeinsamkeiten der CBPR mit den BCR. Denn anders als bei BCR beziehen sich *codes of conduct* i.S.d. § 38a BDSG nicht auf den internationalen Datentransfer. Sie entfalten keine Rechtsverbindlichkeit[22] und die Möglichkeit, *codes of conduct* i.S.d. § 38a BDSG zu erlassen, besteht nur für Vereinigungen, während BCR auf einzelne Unternehmen ausgerichtet sind.

4.2 Inhaltliche Anforderungen

Sowohl bei BCR als auch bei CBPR erlegen sich die Unternehmen selbst Regeln auf, die auf den Bestimmungen des jeweiligen Datenschutzsystems basieren. Die CBPR stützen sich inhaltlich auf die Bestimmungen des *APEC Privacy Frameworks*; die dort aufgeführten Grundsätze stellen Minimalstandards dar, die durch die CBPR erreicht werden müssen.

BCR müssen zu einem Datenschutzniveau führen, das im Wesentlichen dem der DSRL 95/46/EG entspricht. Leitlinien für die inhaltliche Ausgestaltung geben die WP 74, 108, 153[23], 154 und 155 der Art. 29-Gruppe.

4.3 Genehmigungsverfahren

BCR und CBPR ergehen auf freiwilliger Basis durch Initiative der übermittelnden Stelle. Allein an ihr liegt es, Unternehmensrichtlinien zu erstellen und sie der zuständigen Behörde vorzulegen.

CBPR sind wie dargestellt einem *Accountability Agent* zu übermitteln, der ihre Vereinbarkeit mit den geltenden Datenschutzbestimmungen prüft und bei einem positiven Ergebnis die Vereinbarkeit zertifiziert.

19 In Art. 26 Abs. 2 EG-DSRL werden verbindliche Unternehmensrichtlinien anders als in § 4c Abs. 2 BDSG nicht ausdrücklich benannt, aber auch diese Regelung ermöglicht verbindliche Unternehmensrichtlinien als ausreichende Garantie, so fügen sie sich in den unbestimmten Rechtsbegriff der ausreichenden Garantien ein.

20 Vgl. Greenleaf, Asia-Pacific developments in information privacy law, S. 8, 11, abrufbar unter: http://privacy.org.nz/asia-pacific-developments-in-information-privacy-law-and-its-interpretation-graham-greenleaf/.

21 Gola/Schomerus, BDSG (11. Aufl.), § 38a Rn. 1.

22 Gola/Schomerus, BDSG (11. Aufl.), § 38a Rn. 3.

23 Abrufbar unter: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm.

Eine solche Anerkennung durch eine einzelne zuständige Stelle stellvertretend für und unabhängig von anderen EU-Datenschutzbehörden ist bei BCR dagegen nicht möglich; diese ist vielmehr mit höherem bürokratischem Aufwand verbunden. Die Art. 29-Gruppe strebt zumindest eine EU-weite Koordinierung der Datenschutzbehörden ausgehend von einer so genannten *lead authority* an:[24] Danach soll jeweils eine so genannte *lead authority*, d.h. eine einzelne Datenschutzbehörde, ermittelt werden, der das Unternehmen den Entwurf seiner BCR übermittelt. Die *lead authority* soll anhand von Kriterien wie dem Sitz der Hauptniederlassung bzw. des für Datenschutz zuständigen Unternehmensteils ermittelt werden. Sie prüft die vorgelegten BCR daraufhin, ob die verantwortliche Stelle durch die BCR ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte stellt und übermittelt bei positiver Prüfung die Unterlagen an ebenfalls betroffene Datenschutzbehörden anderer Mitgliedstaaten. Soweit Staaten an dem so genannten *mutual recognition*-Verfahren[25] teilnehmen, genügt der Erhalt der Unterlagen, andernfalls hat der andere Mitgliedstaat mitzuteilen, ob dort Vorbehalte gegen eine Anerkennung der BCR bestehen. Werden keine Einwände durch die anderen Behörden erhoben, erfolgt die Anerkennung durch die *lead authority*. Anders als bei den CBPR ist somit die Anerkennung von BCR an weitergehende Abstimmungen der Behörden untereinander gebunden.

Es ist zudem zu beachten, dass in einigen Staaten der EU bzw. in einigen Bundesländern in Deutschland[26] zusätzlich in einem zweiten Schritt eine Genehmigung der einzelnen, auf den BCR basierenden Übermittlung erforderlich ist,[27] wobei weitere nationale Erfordernisse neben das EU-weit koordinierte Anerkennungsverfahren treten können.[28]

Auch bei CBPR können zusätzliche nationale Anforderungen an den Datentransfer bestehen. Da die Verpflichtungen aus den CBPR neben die nationalen Datenschutzverpflichtungen treten, können nationale Datenschutzvorschriften über die Vorgaben der CBPR hinausgehen. Eine zunehmende Zahl der APEC-Mitgliedstaaten hat bindende Datenschutzbestimmungen auf nationaler Ebene erlassen und knüpft in diesen den internationalen Datentransfer an bestimmte Voraussetzungen. Nutzt ein Unternehmen CBPR, so legitimieren diese folglich in solchen Rechtssystemen nicht allein den internationalen Datentransfer, auch Unternehmen mit zertifizierten CBPR müssen sich bei einer Datenübermittlung über staatliche Grenzen hinweg an die nationalen Bestimmungen halten.

4.4 Geltungsbereich

Die Genehmigung der CBPR bezieht sich auf Datentransfers des Unternehmens innerhalb der teilnehmenden APEC-Staaten, wobei nicht nur der Transfer von Daten innerhalb des Unternehmens, sondern auch an Dritte umfasst ist. BCR ermöglichen dagegen die Datenübermittlung in jegliche Drittstaaten, jedoch nur innerhalb einer Unternehmensgruppe.

4.5 Kontrolle und Durchsetzung

Sowohl CBPR als auch BCR sind intern als auch extern rechtlich verbindlich.

Die Kontrolle der Einhaltung der CBPR soll zunächst einmal durch die Unternehmen selbst erfolgen. So haben diese in ihrem Self Assessment bereits Maßnahmen und Vorkehrungen aufzuführen, die eine Umsetzung der Richtlinien sicherstellen sollen und der Kontrolle ihrer Einhaltung dienen sollen. Daneben erfolgt eine Kontrolle durch die *Accountability Agents* und die *Privacy Enforcement Authorities*. Das CPEA zielt zudem darauf ab, eine Kooperation und einen Informationsaustausch der Behörden auch bei der Durchsetzung der CBPR über staatliche Grenzen hinaus sicherzustellen. Die konkrete Ausgestaltung der Durchsetzung und Haftung im Fall des Verstoßes wird aber den Mitgliedstaaten überlassen.

Auch bei BCR soll zunächst einmal eine Kontrolle durch die Unternehmen selbst erfolgen, so sollen in den BCR selbst Maßnahmen genannt werden, die die Umsetzung der BCR und deren Kontrolle sicherstellen sollen, wie Audits, Mitarbeiterschulungen und Beschwerdesysteme.[29] Darüber hinaus wird die Einhaltung auch bei BCR durch die Datenschutzbehörden kontrolliert. Bestimmte Klauseln der BCR sind drittbegünstigend auszugestalten und Betroffenen ist das Recht einzuräumen, wegen Verletzung der BCR Beschwerde bei der Datenschutzbehörde bzw. Klage vor Gericht zu erheben.[30] Nach den Empfehlungen der Art. 29-Gruppe soll in den BCR zudem eine Niederlassung des fraglichen Unternehmens in der EU genannt werden, die für Verstöße gegen die Unternehmensregelungen, die durch verbundene, außerhalb der EU angesiedelte Unternehmensteile erfolgen, die Haftung übernimmt.[31] Diese Niederlassung kann im Fall des Verstoßes gegen BCR eine Schadensersatzpflicht treffen.

5 Fazit und Ausblick

Das *APEC Privacy Framework* sowie die CBPR stellen ein bereits jetzt recht umfassend strukturiertes Datenschutzsystem dar. Zwar wird das durch das *APEC Privacy Framework* begründete Datenschutzniveau oftmals als zu niedrig kritisiert, jedoch wird im Zusammenspiel mit dem neuen CBPR-System durchaus ein einheitlicher, grundlegender Standard für den gesamten APEC-Raum geschaffen. Der tatsächliche Erfolg des Systems in der Praxis bleibt abzuwarten, insbesondere steht in Frage, ob und inwiefern ein ausreichender Anreiz für die Unternehmen besteht, sich dem System anzuschließen. Ein Vorteil des CBPR-Systems ist aber in jedem Falle darin zu sehen, dass der bürokratische Aufwand im Vergleich zu dem der BCR deutlich geringer ist. Entscheidend für den Erfolg des CBPR-Systems dürfte sein, wie konsequent die Mitgliedstaaten die Frage der Kontrolle und Durchsetzung behandeln. Die weitere Entwicklung dieses durchaus viel versprechenden Datenschutzkonzepts sollte auch aufgrund der Ähnlichkeiten mit dem System der BCR und eventuell daraus folgenden Möglichkeiten der Kooperation im Blick behalten werden.

24 Art. 29-Gruppe, WP 107.

25 Beim mutual recognition-Verfahren erfolgt eine gegenseitige Anerkennung der Bewertung der BCR unter Verzicht auf eine eigene Prüfung; derzeit nehmen 21 Nationen an diesem Verfahren teil: Belgien, Bulgarien, Deutschland, Estland, Frankreich, Großbritannien, Island, Irland, Italien, Lettland, Liechtenstein, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Slowakei, Slowenien, Spanien, Tschechische Republik und Zypern.

26 Übersicht unter: http://ec.europa.eu/justice/data-protection/document/international-transfers/files/table_nat_admin_req_en.pdf.

27 Auf den BCR basierenden Datenübermittlungen sollen nach Art. 42 Abs. 3 DS-GVO-E keiner zusätzlichen Genehmigung mehr bedürfen.

28 Filip, Binding Corporate Rules (BCR) aus der Sicht einer Datenschutzaufsichtsbehörde, ZD 2013, 51, 53.

29 Art. 29-Gruppe, WP 154, S. 8 f.

30 Art. 29-Gruppe, WP 153, S. 3 und WP 154, S. 9 f.

31 Art. 29-Gruppe, WP 155, S. 4.