ARTIKEL-29-DATENSCHUTZGRUPPE

538/14/DE
WP 212

Stellungnahme 02/2014 zu einem Regelwerk für die Anforderungen an verbindliche unternehmensinterne Regelungen, die den nationalen Datenschutzbehörden der EU vorgelegt werden, und an Regelungen für den grenzüberschreitenden Datenschutz, die den von der APEC anerkannten „CBPR Accountability Agents“ vorgelegt werden

Angenommen am 27. Februar 2014

Gemeinsame Arbeit von Sachverständigen der Artikel-29-Datenschutzgruppe und der APEC-Länder über ein Regelwerk für die Anforderungen an verbindliche unternehmensinterne Regelungen, die den nationalen Datenschutzbehörden der EU vorgelegt werden, und an Regelungen für den grenzüberschreitenden Datenschutz, die den von der APEC anerkannten „CBPR Accountability Agents" vorgelegt werden

ÜBERBLICK

Ziel des Regelwerks

Das Regelwerk ist als informelle pragmatische Checkliste für Unternehmen gedacht, die die Genehmigung von verbindlichen unternehmensinternen Regelungen (Binding Corporate Rules – BCR) und/oder die Zertifizierung von Regelungen für den grenzüberschreitenden Datenschutz (Cross Border Privacy Rules – CBPR) beantragen. Auf diese Weise erleichtert es die Gestaltung und Annahme von Grundsätzen für den Schutz personenbezogener Daten, die mit jedem der beiden Systeme im Einklang stehen.

Wenngleich es nicht darum geht, mit dem Regelwerk die gegenseitige Anerkennung beider Systeme zu erreichen, so könnte es doch als Grundlage für eine **Doppelzertifizierung** dienen. Auf jeden Fall **bedürfen** die Datenschutzgrundsätze von antragstellenden internationalen Unternehmen, die sowohl im Gebiet der EU als auch im Gebiet der APEC tätig sind, **der Zustimmung** der zuständigen Stellen der EU-Mitgliedstaaten bzw. der APEC-Länder gemäß den geltenden Genehmigungsverfahren.

Hintergrund

Sachverständige der Artikel-29-Datenschutzgruppe der Datenschutzbehörden in der EU (nachstehend „WP29")[1] und der Länder, die der Untergruppe Datenschutz der APEC angehören, haben ein praktisches Instrument ausgearbeitet, um die jeweiligen Anforderungen an die BCR und CBPR (nachstehend „Regelwerk") darzustellen.[2]

In diesem Regelwerk sind die wichtigsten Elemente zusammengefasst, die nach Maßgabe der Anforderungen der nationalen Datenschutzbehörden in der EU und der zuständigen Stellen in den APEC-Ländern in den Datenschutzgrundsätzen enthalten sein müssen, deren Genehmigung als BCR durch die nationalen Datenschutzbehörden der EU gemäß den Datenschutzgesetzen der EU-Mitgliedstaaten bzw. als CBPR gemäß den Vorschriften der APEC-Länder beantragt wird.

[1] Die Artikel-29-Datenschutzgruppe wurde gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr eingesetzt. Sie besteht aus je einem Vertreter der von den einzelnen Mitgliedstaaten bestimmten Kontrollstellen (IES), einem Vertreter des Europäischen Datenschutzbeauftragten und einem Vertreter der Europäischen Kommission. Die Gruppe ist unabhängig und hat beratende Funktion.

[2] In Zukunft können Wirtschaft und Zivilgesellschaft im Einklang mit den Mechanismen der APEC für die Beteiligung von Interessengruppen und den Konsultationsmechanismen der Artikel-29-Datenschutzgruppe einen Beitrag zur Tätigkeit der betreffenden Gremien leisten.

Das Regelwerk wurde von hochrangigen Vertretern der APEC anlässlich ihrer Tagung am 27. und 28. Februar 2014 gebilligt, und die Artikel-29-Datenschutzgruppe nahm auf ihrer Plenartagung am 26. und 27. Februar 2014 eine Stellungnahme/ein Arbeitsdokument an.

Gliederung des Regelwerks

Das Regelwerk umfasst für jeden der wesentlichen Grundsätze bzw. jede der wesentlichen Anforderungen der betreffenden Systeme

- einen „**gemeinsamen Block**“, in dem die wichtigsten gemeinsamen oder ähnlichen Elemente der BCR bzw. der CBPR beschrieben sind;

- „**zusätzliche Blöcke**“, in denen die wichtigsten Unterschiede und zusätzlichen Elemente dargelegt sind, die die BCR bzw. die CBPR auszeichnen.

Wenngleich im gemeinsamen Block gewisse Übereinstimmungen zwischen den obligatorischen Elementen des CBPR- und des BCR-Systems aufgezeigt werden, reicht dies per se nicht aus, eine Zertifizierung von CBPR durch einen von der APEC anerkannten Accountability Agent bzw. eine Genehmigung von BCR durch eine nationale Datenschutzbehörde in der EU zu erlangen. Ein Unternehmen, das eine Genehmigung seiner BCR durch Datenschutzbehörden beantragt, muss darüber hinaus die im zusätzlichen Block für BCR enthaltenen Elemente **berücksichtigen**, und ein Unternehmen, das die Zertifizierung ihrer CBPR durch einen von der APEC anerkannten Accountability Agent beantragt, muss **auch** den im zusätzlichen Block für CBPR enthaltenen Elementen **Rechnung tragen**.

REGELWERK FÜR DIE ANFORDERUNGEN AN VERBINDLICHE UNTERNEHMENSINTERNE REGELUNGEN, DIE DEN NATIONALEN DATENSCHUTZBEHÖRDEN DER EU VORGELEGT WERDEN, UND AN REGELUNGEN FÜR DEN GRENZÜBERSCHREITENDEN DATENSCHUTZ, DIE DEN VON DER APEC ANERKANNTEN „CBPR ACCOUNTABILITY AGENTS“ VORGELEGT WERDEN

ZUSAMMENFASSUNG

Einführung

In diesem Dokument (nachstehend „Regelwerk“) werden die Anforderungen dargelegt, welche im System der verbindlichen unternehmensinternen Regelungen (Binding Corporate Rules, nachstehend „BCR“), die von den Datenschutzbehörden der Mitgliedstaaten der Europäischen Union (nachstehend „EU“) üblicherweise für die unternehmensintern erfolgende Übermittlung personenbezogener Daten in Drittländer genehmigt werden, und im System der Regelungen für den grenzüberschreitenden Datenschutz (Cross Border Privacy Rules, nachstehend „CBPR“) der Asiatisch-Pazifischen Wirtschaftsgemeinschaft (nachstehend „APEC“) übereinstimmen bzw. vergleichbar sind.

Darüber hinaus werden die zusätzlichen Elemente aufgezeigt, die im Hinblick auf das Verfahren zur Genehmigung und Konformitätsüberprüfung der nationalen Datenschutzbehörden in der EU und der von der APEC anerkannten CBPR Accountability Agents für die BCR-Genehmigung bzw. die CBPR-Zertifizierung erforderlich sind. Die Einzelgenehmigungen von BCR durch nationale Datenschutzbehörden gemäß den EU-Datenschutzvorschriften und die Zertifizierung von CBPR durch von der APEC anerkannte Accountability Agents (nachstehend „APEC Accountability Agents“) bleiben davon unberührt. Das gilt auch für die Durchsetzung durch die zuständigen Überwachungs- und/oder Vollzugsbehörden.

Dieses Regelwerk beinhaltet nicht unbedingt eine umfassende Analyse aller BCR- und CBPR-Elemente; es ist auch nicht die einzige Möglichkeit zur Darstellung dieser zwei Systeme und ist weder als rechtlicher Ratgeber noch als Wiedergabe des offiziellen Standpunkts der Organisationen zu verstehen, die an seiner Ausarbeitung beteiligt waren.

Zweck und Gliederung

Dieses Regelwerk zielt darauf ab, Unternehmen bei der Anwendung von Regelungen zum Schutz personenbezogener Daten und der Privatsphäre zu unterstützen und ihnen die Einhaltung der Anforderungen in Bezug auf BCR und CBPR zu erleichtern. Es soll Unternehmen, die Datenschutzgrundsätze ausarbeiten und anwenden möchten, als pragmatische Checkliste für die gleichzeitige Beantragung der Genehmigung von BCR durch nationale Datenschutzbehörden in der EU und der Zertifizierung von CBPR durch einen APEC Accountability Agent dienen.

Unternehmen, die die Genehmigung von BCR durch nationale Datenschutzbehörden in der EU und die Zertifizierung von CBPR durch einen APEC Accountability Agent, d. h. eine Doppelzertifizierung, in Erwägung ziehen, soll das Regelwerk als Vergleichsinstrument dienen. Somit erfolgt eine Gegenüberstellung der BCR- und der CBPR-Anforderungen, die Unternehmen die Ausarbeitung von Regelungen zum Schutz personenbezogener Daten und der Privatsphäre mit Blick auf die Einhaltung der Anforderungen beider Systeme und die Anwendung dieser Regelungen auf ihre Unternehmensteile, Tochtergesellschaften und Zweigniederlassungen (nachstehend „die Unternehmensgruppe“) erleichtern soll. Die förmliche Feststellung der Übereinstimmung mit einem der Systeme kann nur durch die entsprechenden anerkannten, in dem jeweiligen System anwendbaren Verfahren im Einklang mit den Anforderungen erfolgen, die in den geltenden Rahmenbedingungen festgelegt sind.

Dieses Regelwerk ist wie folgt gegliedert: Es umfasst für jeden der darin genannten Grundsätze einen Block übereinstimmender oder ähnlicher Elemente, die sowohl für BCR als auch für CBPR erforderlich sind. Anschließend sind in zusätzlichen Blöcken für die einzelnen Anforderungen Elemente aufgelistet, die in den beiden Systemen unterschiedlich sind. Darüber hinaus können diese zusätzlichen Blöcke Ausnahmen und Klarstellungen in Bezug auf das jeweilige System enthalten. Wenngleich in den gemeinsamen Blöcken gewisse Übereinstimmungen zwischen den im CBPR-System und im BCR-System gleichermaßen vorgeschriebenen Elementen aufgezeigt werden, reichen diese per se nicht aus, eine Zertifizierung von CBPR durch einen von der APEC anerkannten Accountability Agent bzw. eine Genehmigung von BCR durch eine nationale Datenschutzbehörde in der EU zu erlangen. Ein Unternehmen, das eine Genehmigung seiner BCR durch nationale Datenschutzbehörden in der EU beantragt, muss auch die im zusätzlichen Block für BCR enthaltenen Elemente berücksichtigen, und ein Unternehmen, das die Zertifizierung seiner CBPR durch einen APEC Accountability Agent beantragt, muss auch den im zusätzlichen Block für CBPR enthaltenen Elementen Rechnung tragen.

Es sei darauf hingewiesen, dass zwischen den Anforderungen, die von den nationalen Datenschutzbehörden in der EU für die Genehmigung von BCR im Allgemeinen gestellt werden, insbesondere denjenigen, die sich aus den Datenschutzvorschriften der EU ergeben, und den Anforderungen des CBPR-Programms erhebliche Unterschiede bestehen können. Darüber hinaus gibt es Unterschiede zwischen den jeweiligen Zielen, Anwendungsbereichen und Überprüfungsverfahren des BCR- und des CBPR-Systems. Aufgrund dieser Unterschiede sind einige der BCR- bzw. CBPR-Anforderungen nicht vollständig miteinander vereinbar. Daher müssen die antragstellenden Unternehmen, um Konflikte mit dem anwendbaren Recht zu vermeiden, den Anwendungsbereich ihrer Regelungen zum Schutz personenbezogener Daten und der Privatsphäre explizit darlegen. So muss aus dem Antrag deutlich hervorgehen, in welchen Fällen sie EU-Datenschutzvorschriften und/oder Anforderungen des CBPR-Programms der APEC anwenden werden, da die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der EU-Datenschutzvorschriften und/oder der Vorschriften der APEC-Länder erfolgen muss.

Die Regelungen für den Schutz personenbezogener Daten und der Privatsphäre sollten auf Struktur, Datenverarbeitung, Datenschutzgrundsätze und -verfahren der betreffenden Unternehmensgruppe zugeschnitten sein. Daher sei darauf hingewiesen, dass die nationalen Datenschutzbehörden in der EU und die anerkannten CBPR Accountability Agents in der APEC eine wortgetreue Wiedergabe des vorliegenden Rahmens nicht akzeptieren.

Anwendungsbereich

Die Zertifizierung von CBPR ist auf diejenigen Unternehmen beschränkt, die in einem am CBPR-System teilnehmenden Land zertifiziert sind. Der Anwendungsbereich der Zertifizierung der CBPR eines bestimmten Unternehmens erstreckt sich auf die im CBPR-Zertifizierungsantrag genannten Unternehmensteile, Tochtergesellschaften und Zweigniederlassungen.

Jedes Unternehmen, das von EU-Mitgliedstaaten aus personenbezogene Daten an Empfänger in Drittländern übermitteln möchte, kann die Genehmigung seiner BCR bei einer nationalen Datenschutzbehörde in der EU beantragen. Der Anwendungsbereich der BCR eines bestimmten

Unternehmens ist auf die Unternehmensteile, Tochtergesellschaften und Zweigniederlassungen beschränkt, die im Antrag auf Genehmigung der BCR genannt sind. Die ordnungsgemäße Anwendung der genehmigten BCR bietet einen angemessenen Schutz für die Übermittlung von Daten von den (im Antrag des Unternehmens) genannten und in der EU ansässigen Unternehmensteilen zu den darin ebenfalls genannten Unternehmensteilen, Tochtergesellschaften und Zweigniederlassungen in Drittländern.

Die für die grenzüberschreitende Übermittlung personenbezogener Daten geltenden Regelungen für den Schutz personenbezogener Daten und der Privatsphäre können, wenn sie nach den entsprechenden Verfahren genehmigt wurden, zur Unternehmensstrategie für alle personenbezogenen Daten werden, die vom Unternehmen oder von der Unternehmensgruppe gemäß der BCR-Genehmigung der nationalen Datenschutzbehörden in der EU und der CBPR-Zertifizierung der APEC Accountability Agents verarbeitet werden. Im Falle der Verarbeitung[3] personenbezogener Daten in der EU[4] gelten auch die Anforderungen der EU-Datenschutzvorschriften. Für die Verarbeitung personenbezogener Daten in einem APEC-Land gilt das Recht des jeweiligen Landes.

Dieses Regelwerk basiert auf folgenden Dokumenten:

EU:

- Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, nachstehend „**Richtlinie 95/46/EG***“;*

- nationale Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG;

- *Arbeitsdokument: Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer* (WP74), angenommen von der Artikel-29-Datenschutzgruppe am 3. Juni 2003, nachstehend „**WP74**“;

[3] Der Begriff „Verarbeitung“ schließt die Speicherung sowie jeden Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten ein (siehe Artikel 2 Buchstabe b der Richtlinie 95/46/EG).

[4] Die Datenschutzvorschriften der EU-Mitgliedstaaten gelten für die Verarbeitung personenbezogener Daten (einschließlich der Speicherung), die (a) die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet der EU besitzt; (c) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht in der EU niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet der EU belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der EU verwendet werden; (b) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht in der EU aber an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht eines EU-Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet (siehe Artikel 4 Absatz 1 der Richtlinie 95/46/EG).

- *Arbeitsdokument: Muster-Checkliste für Anträge auf Genehmigungen verbindlicher unternehmensinterner Datenschutzregelungen* (WP108), angenommen von der Artikel-29-Datenschutzgruppe am 3. Juni 2003, nachstehend „**WP108**“;

- *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (Empfehlung 1/2007 zum Standardantrag auf Genehmigung verbindlicher unternehmensinterner Regelungen für die Übermittlung personenbezogener Daten)* (WP133), angenommen von der Artikel-29-Datenschutzgruppe am 10. Januar 2007, nachstehend „**WP133**“;

- *Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR)* (WP153), angenommen von der Artikel-29-Datenschutzgruppe am 24. Juni 2008, nachstehend „**WP153**“;

- *Arbeitsdokument : Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)* (WP154), angenommen von der Artikel-29-Datenschutzgruppe am 24. Juni 2008, nachstehend „**WP154**“;

- *Arbeitsdokument zu „Häufig gestellten Fragen“ über verbindliche unternehmensinterne Datenschutzregelungen (BCR)* (WP155), angenommen von der Artikel-29-Datenschutzgruppe am 24. Juni 2008, zuletzt überarbeitet und angenommen am 8. April 2009, nachstehend „**WP155**“.

APEC:

- *APEC Privacy Framework* (APEC-Rechtsrahmen für den Schutz der Privatsphäre), nachstehend „**Privacy Framework**“;

- *APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines* (Grenzüberschreitende(s)Regelsystem, Grundsätze, Vorschriften und Leitlinien der APEC für den Schutz der Privatsphäre), nachstehend „**Policies, Rules and Guidelines**“;

- *APEC Cooperation Arrangement for Cross-Border Privacy Enforcement* (APEC-Abkommen über die grenzüberschreitende Durchsetzung des Datenschutzes), nachstehend „**CPEA**“;

- *Template Notice of Intent to Participate in the APEC Cross-Border Privacy Rules System* (Musterabsichtserklärung für die Teilnahme am grenzüberschreitenden APEC-Regelsystem für den Schutz der Privatsphäre), nachstehend „**Template notice of intent**“;

- *Accountability Agent APEC Recognition Application* (Antrag auf Anerkennung als APEC Accountability Agent), nachstehend „**Recognition application**“;

- *APEC Cross-Border Privacy Rules System Intake Questionnaire* (APEC-Aufnahmefragebogen für das APEC-Regelsystem für den Schutz der Privatsphäre, nachstehend „**Intake Questionnaire**“;

- *APEC Cross-Border Privacy Rules System Program Requirements* (Anforderungen des APEC-Programms mit Regelungen für den grenzüberschreitenden Datenschutz), nachstehend „**Program requirements**“.

Regelwerk zu den Anforderungen an BCR und CBPR in Bezug auf den Schutz personenbezogener Daten und der Privatsphäre

1. Ziel der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Unternehmensinterne Regelungen für den Schutz personenbezogener Daten und der Privatsphäre sollten

- einen angemessenen Schutz der personenbezogenen Daten bieten, die von der betreffenden Unternehmensgruppe übermittelt und verarbeitet werden, wie dies im Rahmen des Verfahrens zur Genehmigung von BCR und des Verfahrens zur Zertifizierung von CBPR vorgeschrieben ist [5]; und
- eine gegenüber dem betreffenden Unternehmen durchsetzbare Verpflichtung darstellen, die Einhaltung der Regelungen für den Schutz personenbezogener Daten und der Privatsphäre sicherzustellen [6] (siehe Abschnitt 3 und Abschnitt 21 des Regelwerks);
- einen Verweis auf die geltenden Rechtsvorschriften zum Datenschutz enthalten [7].

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Unternehmensinterne Regelungen für den Schutz personenbezogener Daten und der Privatsphäre sollten alle Mitglieder und Mitarbeiter der Unternehmensgruppe unmissverständlich dazu verpflichten, die betreffenden Regelungen gemäß den anwendbaren Rechtsvorschriften auszulegen und einzuhalten. [8]	Einzelstaatliche Rechtsvorschriften und Regelungen, die über das hinausgehen, was im Rahmen des CBPR-Systems vorgesehen ist, gelten weiterhin uneingeschränkt. Gehen die Anforderungen des CBPR-Systems über die Anforderungen der einzelstaatlichen Rechtsvorschriften und Regelungen hinaus, so müssen die betreffenden Unternehmen die zusätzlichen Anforderungen freiwillig erfüllen, um an dem System teilzunehmen. Die Datenschutzbehörden des betreffenden Landes sollten jedoch in der Lage sein, im Rahmen der anwendbaren einzelstaatlichen Rechtsvorschriften und Regelungen Durchsetzungsmaßnahmen zum Schutz personenbezogener Daten zu treffen, die mit den Anforderungen des CBPR-Programms im Einklang stehen [9] (*siehe auch Abschnitt 26, Verhältnis zwischen dem einzelstaatlichen Recht und den unternehmensinternen*

	Regelungen für den Schutz personenbezogener Daten und der Privatsphäre).

Quellenangaben

[5] EU: siehe WP74, Abschnitt 3.1, S. 7-9; APEC: siehe Privacy Framework, Part iii, Principle I, Ziffer 14, S. 11.

[6] EU: siehe WP154, Einführung, S. 3 und WP74, S. 10-14; APEC: siehe CBPR Policies, Rules and Guidelines, Ziffer 8, S. 4; CBPR Program Requirements, Ziffern 39 und 40.

[7] EU: siehe WP154, Einführung, S. 3; APEC: siehe Recognition application, Annex A, Ziffer 4, S. 5.

[8] EU: siehe WP74, Abschnitt 3.3.1, S. 10-11; WP153, Ziffer 1.1, S. 3.

[9] APEC: siehe Policies, Rules and Guidelines, Ziffer 44, S. 10.

2. Anwendungsbereich der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Unternehmensinterne Regelungen für den Schutz personenbezogener Daten und der Privatsphäre sollten eine Beschreibung des Anwendungsbereichs dieser Regelungen umfassen, einschließlich

- des geografischen Anwendungsbereichs (siehe Abschnitte 4 und 15 dieses Regelwerks); [10]
- des sachlichen Anwendungsbereichs (d. h. Art der Daten, Kunden/potenzielle Kunden, Mitarbeiter/potenzielle Mitarbeiter, Lieferanten usw.); [11]
- der Liste der Unternehmensteile, die an die Regelungen des betreffenden Unternehmens für den Schutz personenbezogener Daten und der Privatsphäre gebunden sind; [12] und
- des Zwecks der Übermittlung und/oder Verarbeitung. [13]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die Verarbeitung öffentlich zugänglicher personenbezogener Daten unterliegt den Anforderungen der EU-Datenschutzvorschriften und ist nicht von den BCR ausgenommen. Unternehmen, die sich für die Teilnahme am BCR-System entscheiden, müssen die Datenschutzgrundsätze und –praktiken gemäß den Anforderungen des BCR-Programms für alle personenbezogenen Daten umsetzen, die innerhalb der Unternehmensgruppe in Drittländer übermittelt werden. Wenngleich dies für die BCR-Genehmigung nicht erforderlich ist, können die teilnehmenden Unternehmen für alle personenbezogenen Daten, die weltweit innerhalb der Unternehmensgruppe verarbeitet werden, die gleichen Datenschutzgrundsätze und -verfahren anwenden, vorausgesetzt, dass die Einhaltung der EU-Datenschutzvorschriften bei der Verarbeitung personenbezogener Daten in der EU sichergestellt ist.	k. A.
Klarstellung des Anwendungsbereichs der BCR	**Klarstellung des Anwendungsbereichs der CBPR**
k. A.	In einigen Fällen sind die

	unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre nicht auf öffentlich zugängliche Daten anwendbar. [14] Unternehmen, die sich für die Teilnahme am CBPR-System entscheiden, sollten die Datenschutzgrundsätze und –praktiken gemäß den Anforderungen des CBPR-Programms für alle personenbezogenen Daten umsetzen, die sie erhoben oder erhalten haben und die grenzüberschreitend an andere teilnehmende APEC-Länder übermittelt werden. Wenngleich dies im Rahmen des CBPR-Systems nicht erforderlich ist, wird den teilnehmenden Unternehmen nahegelegt, für alle personenbezogenen Daten, die sie erhoben oder erhalten haben, die gleichen Datenschutzgrundsätze und –verfahren anzuwenden, selbst wenn diese nicht grenzüberschreitend oder nur außerhalb der teilnehmenden APEC-Länder grenzüberschreitend übermittelt werden. [15]

Quellenangaben

[10] EU: siehe WP153, Abschnitt 4.2 und WP108, Abschnitte 7.1 und 7.2, S. 7-8; APEC: siehe Intake Questionnaire, v-vi, S. 2-3.

[11] EU: siehe WP153, Abschnitt 4.2 und WP108, Abschnitte 7.1.1 und 7.2, S. 7-8; APEC: siehe Intake Questionnaire, iv, S. 2.

[12] EU: siehe WP153 Abschnitt 6.2; WP108, Abschnitt 7.1.3, S. 8; APEC: siehe Intake Questionnaire, ii, S. 2.

[13] EU: siehe WP153 Abschnitt 4.1; WP108, Abschnitt 7.1.2, S. 8; APEC: siehe CBPR Program Requirement, 1 b) und 1 c).

[14] APEC: siehe APEC Privacy Framework, Ziffer 11, S. 7.

[15] APEC: siehe Policies, Rules and Guidelines, Ziffer 8, S. 4.

3. Durchsetzbare Verpflichtung innerhalb eines Unternehmens

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Alle Unternehmensteile einer Gruppe, die eine Genehmigung von BCR durch eine nationale Datenschutzbehörde in der EU bzw. die Zertifizierung von CBPR durch einen von der APEC anerkannten Accountability Agent anstreben, müssen einer durchsetzbaren Verpflichtung zur Einhaltung der in dem Unternehmen geltenden Regelungen für den Schutz personenbezogener Daten und der Privatsphäre gemäß den geltenden Rechtsvorschriften unterliegen, die gegebenenfalls von einzelnen betroffenen Personen und von der Regulierungsstelle geltend gemacht werden kann. [16]

Zusätzliche Elemente für die BCR-Genehmigung: Verbindlichkeit innerhalb einer Unternehmensgruppe (BCR)	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen in den Unternehmensteilen der Gruppe durch eines oder mehrere der nachstehend genannten Instrumente rechtsverbindlich gemacht werden: [17] i) Maßnahmen oder Regeln, die für alle Mitglieder der Unternehmensgruppe rechtsverbindlich sind; ii) Verträge zwischen den Mitgliedern der Unternehmensgruppe; iii) einseitige Erklärungen oder Verpflichtungen seitens des Mutterunternehmens, die für die übrigen Unternehmensteile verbindlich sind; [18] iii) Aufnahme anderer Kontrollmaßnahmen, z. B. von in Gesetzesvorschriften enthaltenen Verpflichtungen, in einem festgelegten rechtlichen Rahmen; iv) Aufnahme der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre in die allgemeinen Unternehmensgrundsätze mit entsprechenden Verhaltensregeln, Audits	k. A.

und Sanktionen zu ihrer Durchsetzung; v) andere Maßnahmen. [19] Darüber hinaus müssen die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre durch eines oder mehrere der nachstehend genannten Instrumente auch für die Beschäftigten rechtsverbindlich gemacht werden: [20] i) individuelle Vereinbarung/ Verpflichtung mit Sanktionen; ii) Klausel in Arbeitsverträgen mit Sanktionen; iii) interne Unternehmensgrundsätze mit Sanktionen; iv) tarifvertragliche Vereinbarungen mit Sanktionen.	
Klarstellung der Verbindlichkeit für ein Unternehmen (BCR) k. A.	**Klarstellung der Rechenschaftspflicht eines Unternehmens (CBPR)** Unternehmen müssen ihrer Rechenschaftspflicht nachkommen, indem sie die Durchsetzbarkeit ihrer Regelungen für den Schutz personenbezogener Daten und der Privatsphäre durch eines oder mehrere der nachstehend genannten Instrumente nachweisen: [21] i) interne Leitlinien oder Grundsätze; ii) Verträge; iii) Einhaltung der geltenden branchen- oder sektorspezifischen Rechtsvorschriften und Regelungen; iv) andere Maßnahmen. Darüber hinaus müssen die Unternehmen für die Mitarbeiterschulung in Bezug auf die Regelungen für den Schutz personenbezogener Daten und der Privatsphäre sorgen. [22]

Quellenangaben

[16] EU: siehe WP153, Abschnitt 1.1 und 1.2; WP74, Abschnitt 3.3.1, S. 10-11; APEC: siehe Program requirements, Frage 39, S. 24; Anhänge A und B.

[17] EU: siehe WP153, Abschnitt 1.2., Ziffer i, S. 3; WP108, Abschnitt 5.6, S. 5.

[18] In einigen EU-Mitgliedstaaten gelten einfache einseitige Erklärungen gemäß den zivil- und verwaltungsrechtlichen Vorschriften nicht als rechtsverbindlich. In diesen Fällen werden nur Verträge als verbindlich angesehen. Daher sollten sich Unternehmen, die auf andere rechtliche Mittel als Verträge zurückgreifen möchten, vor Ort beraten lassen.

[19] EU: WP74, Abschnitt 3.3.1, S. 10-11; WP153, Abschnitt 1.1, S. 3.

[20] EU: siehe WP74, Abschnitt 3.3.1, S. 10-11; WP 153, Abschnitt 1.1, S. 3 und Abschnitt 1.2., Ziffer ii, S. 3.

[21] APEC: siehe Program requirements, Frage 39, S. 24; Frage 46, S. 26; Anhänge A und B.

[22] APEC: siehe Program requirements, Frage 44, S. 25-26.

4. Rechtsbehelfe für betroffene Personen und Drittbegünstigungsrechte

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

k. A.

Für die Genehmigung von BCR erforderliche Elemente	**Für die Zertifizierung von CBPR erforderliche Elemente**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen den betroffenen Personen als Drittbegünstigten klar und deutlich Durchsetzungsrechte einräumen. Sie müssen konkrete, zugängliche und wirksame Rechtsbehelfe bei Verstoß gegen die Regelungen für den Schutz personenbezogener Daten und der Privatsphäre und Schadenersatzansprüche aufzeigen (siehe Artikel 22 und 23 der Richtlinie 95/46/EG). [23] Darüber hinaus müssen die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre eine Erklärung enthalten, nach der die betroffenen Personen ihre Beschwerde nach Wahl einlegen können - am Gerichtsstand des in der EU ansässigen Datenexporteurs oder - am Gerichtsstand der EU-Hauptniederlassung/des haftenden Unternehmens in der EU oder - bei der zuständigen nationalen Datenschutzbehörde in der EU. Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen darüber hinaus die Zusicherung enthalten, dass die Drittbegünstigungsklausel für alle betroffenen Personen, die Rechte als Drittbegünstigte in Anspruch nehmen können, leicht zugänglich ist. [24]	Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine Erklärung enthalten, nach der sie von den betroffenen Personen wie folgt durchgesetzt werden können: - durch das Beschwerdeverfahren der für die Verarbeitung verantwortlichen Stelle [25] oder - das Streitbeilegungsverfahren des APEC Accountability Agents. [26] Darüber hinaus müssen die betroffenen Personen die Möglichkeit haben, direkt beim gemeinsamen Aufsichtsgremium Beschwerde gegen einen APEC Accountability Agent einzulegen. [27] Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen auch eine Anforderung enthalten, nach der die betroffenen Personen Beschwerde bei APEC Accountability Agents einlegen können. [28] Je nach dem am CBPR-System teilnehmenden Land können die betroffenen Personen im Rahmen der einzelstaatlichen Datenschutzvorschriften über ein privates Klagerecht verfügen, das dazu genutzt werden kann, die Einhaltung der CBPR durchzusetzen.

Quellenangaben

[23] EU: siehe WP74, Abschnitt 3.3.2, S. 11-13.

[24] EU: siehe WP153, Abschnitt 1.7, S. 5.

[25] APEC: siehe Intake Questionnaire, Fragen 41-43, S. 21-22.

[26] APEC: siehe Recognition application, Annex A, Ziffern 9 und 10, S. 7.

[27] APEC: siehe Policies, Rules and Guidelines, Ziffer 35, S. 9.

[28] APEC: siehe Recognition application, Annex A, Ziffern 9 und 10, S. 7.

5. Haftung

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen grundsätzlich vorsehen, dass die Haftung bei einem Unternehmensteil liegt. [29]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen auch eine Selbstverpflichtung dahingehend enthalten, dass [30] - die EU-Hauptniederlassung bzw. das haftende Unternehmen in der EU die Haftung für Handlungen anderer Gruppenmitglieder außerhalb der EU übernimmt und die notwendigen Maßnahmen ergreift, um Verstößen gegen die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre abzuhelfen und Ersatz für Schäden zu leisten, die aus einem Verstoß gegen die Regelungen durch ein Mitglied der Unternehmensgruppe entstanden sind. - Die Beweislast trägt entweder die EU-Hauptniederlassung oder das haftende Unternehmen in der EU, d. h. ihnen obliegt es nachzuweisen, dass der Verstoß, mit dem die betroffene Person ihre Schadenersatzforderung begründet, nicht dem außerhalb der EU ansässigen Mitglied der Unternehmensgruppe zuzurechnen ist. Die EU-Hauptniederlassung bzw. das haftende Unternehmen in der EU kann sich von der Haftung befreien, wenn es nachweist, dass die schadensbegründende Handlung nicht dem außerhalb der EU ansässigen Mitglied der Unternehmensgruppe	Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen auch eine Selbstverpflichtung dahingehend enthalten, dass die Haftung bei dem CBPR-zertifizierten Unternehmensteil liegt. Das ersetzt jedoch nicht eine eventuelle zusätzliche Haftung von Tochtergesellschaften/Zweigniederlassungen nach dem einzelstaatlichen Recht des Landes, in dem ein Verstoß stattgefunden hat.

zuzurechnen ist. Ist es bei Unternehmensgruppen mit einer besonderen Struktur nicht möglich, einem Unternehmensteil der Gruppe die Haftung für außerhalb der EU begangene Verstöße gegen die BCR aufzuerlegen, können die nationalen Datenschutzbehörden im Einzelfall alternative Haftungslösungen akzeptieren, wenn der Antragsteller hinreichende Garantien bietet, dass die Rechte der Betroffenen durchsetzbar sind und dass diese bei der Durchsetzung ihrer Rechte nicht benachteiligt werden. [31]	

Quellenangaben

[29] EU: siehe WP74, Abschnitt 5.5.2, S. 18-19; APEC: siehe Intake Questionnaire, Ziffer ii, S. 2.

[30] EU: siehe WP74, Abschnitt 5.5.2, S. 18-19.

[31] Eine Möglichkeit bestünde in einer gesamtschuldnerischen Haftung der Datenimporteure und -exporteure wie in den EU-Standardvertragsklauseln 2001/497/EG vom 15. Juni 2001 oder in einer alternativen Haftungsregelung auf der Grundlage von Sorgfaltspflichten wie in den EU-Standardvertragsklauseln 2004/915/EG vom 27. Dezember 2004 festgelegt. Insbesondere bei der Weitergabe von Daten von für die Verarbeitung Verantwortlichen an Auftragsverarbeiter käme auch die Anwendung einer Haftungsregelung auf der Grundlage der Standardvertragsklauseln 2002/16/EG vom 27. Dezember 2001 in Frage.

6. Durchsetzbare Verpflichtungen in Bezug auf die Übermittlung von Daten an Dritte

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine durchsetzbare Verpflichtung enthalten, nach der Daten nur an Dritte übertragen werden, die bei der Verarbeitung personenbezogener Daten Schutzmaßnahmen ergreifen, sowie eine Erklärung darüber, wie die Durchsetzung der einschlägigen unternehmensinternen Regelungen gegenüber den Empfängern von Daten in dem betreffenden Land gewährleistet wird. [32]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen Bestimmungen zur Beschränkung des Datentransfers und der Weiterübermittlung außerhalb der Unternehmensgruppe sowie eine Selbstverpflichtung folgenden Inhalts enthalten: [33] - Mit externen Datenverarbeitern innerhalb der EU oder in einem Land mit einem von der Europäischen Kommission anerkannten angemessenen Datenschutzniveau wird schriftlich vereinbart, dass sie nur auf Weisung des für die Verarbeitung Verantwortlichen handeln und für die Durchführung geeigneter Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit der Datenverarbeitung verantwortlich sind. - Bei der Übermittlung von Daten an externe für die Verarbeitung verantwortliche Personen außerhalb der EU und nicht in einem Land mit einem von der Europäischen Kommission anerkannten Datenschutzniveau sind die EU-Vorschriften für den grenzüberschreitenden Datenverkehr zu beachten (Artikel 25 und 26 der	k. A.

Richtlinie 95/46/EG: z. B. durch Bezugnahme auf die von der EU-Kommission gebilligten EU-Standardvertragsklauseln 2001/497/EG oder 2004/915/EG oder durch andere geeignete vertragliche Vereinbarungen nach Maßgabe der Artikel 25 und 26 der EU-Richtlinie). - Bei der Übermittlung von Daten an externe Verarbeiter außerhalb der EU sind zusätzlich zu den Vorschriften für den grenzüberschreitenden Datenverkehr (Artikel 25 und 26 der Richtlinie 95/46/EG) die Vorschriften für Datenverarbeiter zu beachten (Artikel 16 und 17 der Richtlinie 95/46/EG).	
Klarstellung der Verbindlichkeit für Dritte (BCR) k. A.	**Klarstellung der Rechenschaftspflicht bei der Übermittlung an Dritte (CBPR)** Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine Erklärung zu der Frage enthalten, wie personenbezogene Daten geschützt werden, wenn ein Verarbeiter, Agent, Auftragnehmer oder anderer Dienstleister in Anspruch genommen wird, insbesondere unter Beachtung folgender Grundsätze: - Der für die Verarbeitung Verantwortliche muss einen Datenverarbeiter, Agenten, Auftragnehmer oder sonstigen Dienstleister auswählen, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen. [34] - Der für die Verarbeitung Verantwortliche stellt gegenüber dem

	Verarbeiter insbesondere klar, dass i) der Verarbeiter, Agent, Auftragnehmer oder sonstige Dienstleister nur auf Weisung des für die Verarbeitung Verantwortlichen handelt; [35] ii) die Vorschriften für die Sicherheit und Vertraulichkeit auch für den Verarbeiter, Agenten, Auftragnehmer oder sonstigen Dienstleister gelten. [36] Unternehmensinterne Regelungen für den Schutz personenbezogener Daten und der Privatsphäre können durch eines der nachstehend genannten Instrumente für verbindlich erklärt werden: [37] i) interne Leitlinien oder Grundsätze; ii) Verträge; iii) Einhaltung der geltenden branchen- oder sektorspezifischen Rechtsvorschriften und Regelungen; iv) andere Maßnahmen.

Quellenangaben

[32] EU: siehe WP74, Abschnitt 3.2, S. 9-10; APEC: siehe Program requirements, Frage 39, S. 24; Frage 46, S. 26; Anhänge A und B; Intake Questionnaire, Frage 47, S. 22.

[33] EU: siehe WP153, Abschnitt 6.1, Ziffer vi); WP154, Abschnitt 12, S. 7.

[34] APEC: siehe Intake Questionnaire, Frage 35, S. 15.

[35] APEC: siehe Intake Questionnaire, Frage 47-48, S. 22-23.

[36] APEC: siehe Intake Questionnaire, Frage 35, S. 15-16.

[37] APEC: siehe Program requirements, Frage 39, S. 24; Frage 46, S. 26; Anhänge A und B.

7. Verhältnis zu Datenverarbeitern, die der Unternehmensgruppe angehören

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine Erklärung zu der Frage enthalten, wie personenbezogene Daten geschützt werden, wenn der Verarbeiter der Unternehmensgruppe angehört, insbesondere unter Beachtung folgender Grundsätze: [38]

- Der für die Verarbeitung Verantwortliche muss einen Datenverarbeiter auswählen, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen eine ausreichende Gewähr bietet, und er muss für die Einhaltung dieser Maßnahmen sorgen. [39]
- Der für die Verarbeitung Verantwortliche stellt gegenüber dem Verarbeiter insbesondere klar,
  - dass der Verarbeiter nur auf Weisung des für die Verarbeitung Verantwortlichen handelt; [40]
  - die Vorschriften für die Sicherheit und Vertraulichkeit auch für den Verarbeiter gelten. [41]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen die Verpflichtung vorsehen, dass Weisungen schriftlich durch vertragliche Vereinbarungen gemäß dem anwendbaren Recht erteilt werden. [42]	Wenn der für die Verarbeitung Verantwortliche beabsichtigt, personenbezogene Daten an Verarbeiter, Agenten, Auftragnehmer oder sonstige Dienstleister zu übermitteln, so muss er dafür die Einwilligung der betroffenen Person einholen oder seiner Sorgfaltspflicht nachkommen bzw. angemessene Maßnahmen treffen, um sicherzustellen, dass der Betreffende oder das Unternehmen, dem die Daten übermittelt werden, diese gemäß den unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre schützt. [43] Ist es unzweckmäßig bzw. unmöglich, der Sorgfaltspflicht nachzukommen und angemessene Maßnahmen zu treffen, um die Einhaltung der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre sicherzustellen, so legt der für

	die Verarbeitung Verantwortliche eine Begründung vor und beschreibt die anderen Mittel, die genutzt werden, um den Schutz der Daten gemäß den Datenschutzgrundsätzen der APEC dennoch zu gewährleisten. Der für die Verarbeitung Verantwortliche kann mithilfe der nachstehend genannten Instrumente Weisungen erteilen: [44] - interne Leitlinien oder Grundsätze oder - Verträge oder - Einhaltung der geltenden branchen- oder sektorspezifischen Rechtsvorschriften und Regelungen oder - Einhaltung des Kodex und/oder der Vorschriften einer Selbstregulierungsorganisation oder - andere Maßnahmen. In den betreffenden Vereinbarungen muss generell festgelegt sein, dass Verarbeiter, Agenten, Auftragnehmer oder sonstige Dienstleister, die personenbezogene Daten verarbeiten [45] durch die nachstehend genannten Möglichkeiten für einen angemessenen Schutz sorgen: - Einhaltung der mit den APEC-Vorschriften im Einklang stehenden Datenschutzgrundsätze und –maßnahmen gemäß der Datenschutzerklärung des für die Verarbeitung Verantwortlichen; - Umsetzung von Datenschutzmaßnahmen, die im Wesentlichen den Datenschutzgrundsätzen oder -maßnahmen entsprechen, die in der Datenschutzerklärung des für die Verarbeitung Verantwortlichen festgelegt sind; - Befolgung der Weisungen des für die Verarbeitung Verantwortlichen in Bezug auf die Art und Weise, in der mit dessen personenbezogenen Daten umzugehen ist; - Festlegung von Beschränkungen, nach

	denen die Weitervergabe an Nachunternehmer der Einwilligung des für die Verarbeitung Verantwortlichen bedarf; - Zertifizierung der CBPR durch einen APEC Accountability Agent in dem betreffenden Land; Verarbeiter, Agenten, Auftragnehmer oder sonstige Dienstleister setzen den für die Verarbeitung Verantwortlichen davon in Kenntnis, wenn ihnen eine Verletzung der Privatsphäre oder der Sicherheit personenbezogener Daten des für die Verarbeitung Verantwortlichen bekannt wird. [46] Verarbeiter, Agenten, Auftragnehmer oder sonstige Dienstleister treffen unverzüglich Maßnahmen zur Behebung/Bekämpfung des Sicherheitsproblems, das die Datenschutz- oder Sicherheitsverletzung verursacht hat. [47] Verarbeiter, Agenten, Auftragnehmer oder sonstige Dienstleister legen dem für die Verarbeitung Verantwortlichen Selbsteinschätzungen in Bezug auf die Einhaltung der von diesem erteilten Weisungen und/oder der mit diesem geschlossenen Vereinbarungen/Verträge vor. [48] Um die Einhaltung seiner Weisungen und/oder der Vereinbarungen/Verträge sicherzustellen, kontrolliert und überwacht der für die Verarbeitung Verantwortliche regelmäßig und stichprobenartig die Verarbeiter, Agenten, Auftragnehmer oder sonstigen Dienstleister, die von ihm mit der Verarbeitung personenbezogener Daten beauftragt wurden. [49]

Quellenangaben

[38] EU: siehe Richtlinie 95/46/EG, Artikel 17 Absatz 2; WP154, Abschnitt 11, S. 6-7.

[39] APEC: siehe Intake Questionnaire, Frage 35, S. 15.

[40] APEC: siehe Intake Questionnaire, Fragen 47-48, S. 22-23.

[41] APEC: siehe Intake Questionnaire, Frage 35, S. 15-16.

[42] EU: siehe Richtlinie 95/46/EG, Artikel 17 Absatz 2; WP154, Abschnitt 11, S. 6-7.

[43] APEC: siehe Privacy Framework, Part iii, Principle IX, Ziffer 26, S. 28.

[44] APEC: siehe Intake Questionnaire, Frage 46, S. 22.

[45] APEC: siehe Intake Questionnaire, Frage 47-S. 22-23.

[46] APEC: siehe Intake Questionnaire, Frage 35 b), S. 15.

[47] APEC: siehe Intake Questionnaire, Frage 35 c), S. 16.

[48] APEC: siehe Intake Questionnaire, Frage 48, S. 23.

[49] APEC: siehe Intake Questionnaire, Frage 49, S. 23.

8. Beschränkung des Datentransfers und der Weiterübermittlung an Datenverarbeiter und für die Verarbeitung Verantwortliche, die nicht der Unternehmensgruppe angehören

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen die Anforderung enthalten, dass Auftragnehmer, denen Daten zur Verarbeitung übermittelt werden, personenbezogene Daten gemäß den einschlägigen Regelungen des betreffenden Unternehmens schützen. [50]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen auch eine Erläuterung der Maßnahmen zur Beschränkung der Übermittlung und Weiterübermittlung von personenbezogenen Daten außerhalb der Unternehmensgruppe sowie eine Selbstverpflichtung folgenden Inhalts enthalten: - Mit externen Datenverarbeitern innerhalb der EU oder in einem Land mit einem von der Europäischen Kommission anerkannten angemessenen Datenschutzniveau wird schriftlich vereinbart, dass sie nur auf Weisung des für die Verarbeitung Verantwortlichen handeln und für die Durchführung geeigneter Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit der Datenverarbeitung verantwortlich sind. [51] - Bei der Übermittlung von Daten an externe für die Verarbeitung verantwortliche Personen außerhalb der EU und nicht in einem Land mit einem von der Europäischen Kommission anerkannten Datenschutzniveau sind die EU-Vorschriften für den grenzüberschreitenden Datenverkehr zu beachten (Artikel 25 und 26 der	Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen auch eine Erläuterung enthalten, wie personenbezogene Daten geschützt werden, wenn ein Verarbeiter, Agent, Auftragnehmer oder anderer Dienstleister in Anspruch genommen wird. Sie müssen insbesondere Folgendes vorsehen: - Der für die Verarbeitung Verantwortliche muss einen Datenverarbeiter, Agenten, Auftragnehmer oder sonstigen Dienstleister auswählen, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen. [54] - Der für die Verarbeitung Verantwortliche hat gegenüber dem Verarbeiter insbesondere klarzustellen, dass i) dieser nur auf Weisung des für die Verarbeitung Verantwortlichen handelt; [55] ii) die Vorschriften für die Sicherheit und Vertraulichkeit einzuhalten hat, die für den Verarbeiter, Agenten,

Richtlinie 95/46/EG: z. B. durch Bezugnahme auf die von der EU-Kommission gebilligten EU-Standardvertragsklauseln 2001/497/EG oder 2004/915/EG oder durch andere geeignete vertragliche Vereinbarungen nach Maßgabe der Artikel 25 und 26 der EU-Richtlinie). [52] - Bei der Übermittlung von Daten an externe Verarbeiter außerhalb der EU sind zusätzlich zu den Vorschriften für den grenzüberschreitenden Datenverkehr (Artikel 25 und 26 der Richtlinie 95/46/EG) die Vorschriften für Datenverarbeiter zu beachten (Artikel 16 und 17 der Richtlinie 95/46/EG). [53]	Auftragnehmer oder sonstigen Dienstleister gelten. [56] Der für die Verarbeitung Verantwortliche kann mithilfe der nachstehend genannten Instrumente Weisungen erteilen: [57] - interne Leitlinien oder Grundsätze oder - Verträge oder - Einhaltung der geltenden branchen- oder sektorspezifischen Rechtsvorschriften und Regelungen oder - Einhaltung des Kodex und/oder der Vorschriften einer Selbstregulierungsorganisation oder - andere Maßnahmen. In den betreffenden Vereinbarungen muss generell festgelegt sein, dass Verarbeiter, Agenten, Auftragnehmer oder sonstige Dienstleister, die personenbezogene Daten verarbeiten, durch die nachstehend genannten Möglichkeiten für einen angemessenen Schutz sorgen: [58] - Einhaltung der mit den APEC-Vorschriften im Einklang stehenden Datenschutzgrundsätzen und -maßnahmen gemäß der Datenschutzerklärung des für die Verarbeitung Verantwortlichen; - Umsetzung von Datenschutzmaßnahmen, die im Wesentlichen den Datenschutzgrundsätzen oder -maßnahmen entsprechen, die in der Datenschutzerklärung des für die Verarbeitung Verantwortlichen festgelegt sind; - Befolgung der Weisungen des für die Verarbeitung Verantwortlichen in Bezug auf die Art und Weise, in der mit dessen personenbezogenen Daten umzugehen ist; - Festlegung von Beschränkungen, nach denen die Weitervergabe an Nachunternehmer der Einwilligung des

	für die Verarbeitung Verantwortlichen bedarf; - Zertifizierung der CBPR durch einen APEC Accountability Agent in dem betreffenden Land; - andere Maßnahmen. Verarbeiter, Agenten, Auftragnehmer oder sonstige Dienstleister setzen den für die Verarbeitung Verantwortlichen davon in Kenntnis, wenn ihnen eine Verletzung der Privatsphäre oder der Sicherheit personenbezogener Daten des für die Verarbeitung Verantwortlichen bekannt wird. [59] Verarbeiter, Agenten, Auftragnehmer oder sonstige Dienstleister treffen unverzüglich Maßnahmen zur Behebung/Bekämpfung des Sicherheitsproblems, das die Datenschutz- oder Sicherheitsverletzung verursacht hat. [60] Verarbeiter, Agenten, Auftragnehmer oder sonstige Dienstleister legen dem für die Verarbeitung Verantwortlichen Selbsteinschätzungen in Bezug auf die Einhaltung des von diesem erteilten Weisungen und/oder der mit diesem geschlossenen Vereinbarungen/Verträge vor. [61] Um die Einhaltung seiner Weisungen und/oder der Vereinbarungen/Verträge sicherzustellen, kontrolliert und überwacht der für die Verarbeitung Verantwortliche regelmäßig und stichprobenartig die Verarbeiter, Agenten, Auftragnehmer oder sonstigen Dienstleister, die von ihm mit der Verarbeitung personenbezogener Daten beauftragt wurden. [62]

Quellenangaben

[50] EU: siehe WP74, Abschnitt 3.2, S. 9-10; APEC: siehe Intake Questionnaire, Frage 47, S. 22.

[51] EU: siehe Richtlinie 95/46/EG, Artikel 17 Absatz 2; WP154, Abschnitt 12, S. 7.

[52] EU: siehe WP74, Abschnitt 3.2, S. 9-10.

[53] EU: siehe WP154, Abschnitt 12, S. 7.

[54] APEC: siehe Intake Questionnaire, Frage 35, S. 15.

[55] APEC: siehe Intake Questionnaire, Fragen 47-48, S. 22-23.

[56] APEC: siehe Intake Questionnaire, Frage 35, S. 15-16.

[57] APEC: siehe Intake Questionnaire, Frage 46, S. 22.

[58] APEC: siehe Intake Questionnaire, Frage 47, S. 22-23.

[59] APEC: siehe Intake Questionnaire, Frage 35 b), S. 15.

[60] APEC: siehe Intake Questionnaire, Frage 35 c), S. 16.

[61] APEC: siehe Intake Questionnaire, Frage 48, S. 23.

[62] APEC: siehe Intake Questionnaire, Frage 49, S. 23.

9. Begriffsbestimmungen

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Es wird erwartet, dass die Unternehmen ihre Regelungen für den Schutz personenbezogener Daten und der Privatsphäre gemäß den anwendbaren EU-Rechtsvorschriften, insbesondere der Richtlinie 95/46/EG und der Richtlinie 2002/58/EG, den anwendbaren Rechtsvorschriften der am CBPR-System teilnehmenden Länder und dem CBPR-Glossar der APEC auslegen. [63]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine Selbstverpflichtung zur Auslegung der BCR im Sinne der anwendbaren EU-Rechtsvorschriften, insbesondere der Richtlinien 95/46/EG und 2002/58/EG sowie eine Erläuterung der wichtigsten Begriffe enthalten: personenbezogene Daten [64]; für die Verarbeitung Verantwortlicher [65]; Auftragsverarbeiter [66]; betroffene Personen [67]; sensible personenbezogene Daten [68]; Verarbeitung [69]; Dritter [70] und EU-Datenschutzbehörden [71].	k. A.

Quellenangaben

[63] EU: siehe WP154, Abschnitt 2, S. 4; WP155, Frage 8, S. 5; APEC: siehe CBPR Glossary.

[64] EU: siehe Richtlinie 95/46/EG, Artikel 2 Buchstabe a.

[65] EU: siehe Richtlinie 95/46/EG, Artikel 2 Buchstabe d.

[66] EU: siehe Richtlinie 95/46/EG, Artikel 2 Buchstabe e.

[67] EU: siehe Richtlinie 95/46/EG, Artikel 2 Buchstabe a.

[68] EU: siehe Richtlinie 95/46/EG, Artikel 8.

[69] EU: siehe Richtlinie 95/46/EG, Artikel 2 Buchstabe b.

[70] EU: siehe Richtlinie 95/46/EG, Artikel 2 Buchstabe f.

[71] EU: siehe Richtlinie 95/46/EG, Artikel 2 Buchstabe f.

10. Erhebung, Verarbeitung und Verwendung personenbezogener Daten

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen vorsehen, dass personenbezogene Daten gemäß den Festlegungen der anwendbaren Rechtsvorschriften ausschließlich nach Treu und Glauben [72] und auf rechtmäßige Weise für bestimmte Zwecke erhoben und verarbeitet und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden [73].

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen außerdem vorsehen, dass der Zweck der Verarbeitung und Übermittlung personenbezogener Daten eindeutig und rechtmäßig sein muss. [74]	k. A.
Klarstellung der Verarbeitung personenbezogener Daten (BCR)	**Klarstellung der Nutzung personenbezogener Daten (CBPR)**
k. A.	Personenbezogene Daten können mit dem Einverständnis der betroffenen Person für andere kompatible oder verbundene Zweckbestimmungen verwendet werden, wenn dies für die Bereitstellung einer von der betroffenen Person bestellten Dienstleistung oder eines entsprechenden Produkts erforderlich ist oder wenn es nach dem Gesetz und anderen rechtswirksamen Rechtsinstrumenten, Erklärungen und Verkündungen zulässig ist. [75]

Quellenangaben

[72] EU: siehe Richtlinie 95/46/EG, Artikel 6 Absatz 1 Buchstabe a; WP108, Abschnitt 8.2.1, S. 8; WP153, Abschnitt 6.1. Ziffer i, S. 10; WP154, Abschnitt 5, S. 4, Abschnitt 6, S. 5; APEC: siehe Privacy Framework, Part iii, Principle III, Ziffer 18, S. 15; Program Requirements, Frage 7, S. 7.

[73] EU: siehe Richtlinie 95/46/EG, Artikel 6 Absatz 1 Buchstabe b; WP108, Abschnitt 8.2.2, S. 8; WP153, Abschnitt 6.1. Ziffer ii, S. 10; WP154, Abschnitt 3, S. 4; APEC: siehe Privacy Framework, Part iii, Principles III und IV, Ziffern 18 und 19, S. 15-16, Program Requirements, Frage 6 und Frage 8, S. 6 und 8.

[74] EU: siehe Richtlinie 95/46/EG, Artikel 6 Absatz 1 Buchstabe b; WP108, Abschnitt 8.2.2, S. 8; WP153, Abschnitt 6.1. Ziffer ii, S. 10; WP154, Abschnitt 3, S. 4.

[75] APEC: siehe Privacy Framework, Part iii, Principle IV, Ziffer 19, S. 16-17, Program Requirements, Frage 9 und Frage 13, S. 8-10.

11. Datenqualität und –verhältnismäßigkeit / Integrität

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine Selbstverpflichtung enthalten, dass

- personenbezogene Daten sachlich richtig, vollständig und, wenn nötig, auf den neuesten Stand gebracht sind. Darüber hinaus müssen die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre eine Selbstverpflichtung enthalten, dass entsprechende Berichtigungen gegebenenfalls den Beteiligten mitgeteilt werden; [76]
- personenbezogene Daten sachlich richtig sind und den Zwecken entsprechen, für die sie übermittelt und/oder weiterverarbeitet. [77]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen darüber hinaus ausdrücklich die Anforderung enthalten, dass personenbezogene Daten nicht über die Zwecke hinausgehen, für die sie übermittelt und weiterverarbeitet werden. [78] Ferner müssen unternehmensinterne Regelungen für den Schutz personenbezogener Daten und der Privatsphäre die Anforderung enthalten, dass personenbezogene Daten nicht über einen längeren Zeitraum verarbeitet werden, als es für die Realisierung der Zwecke, für die sie erhoben oder gegebenenfalls weiterverarbeitet werden, erforderlich ist. [79]	k. A.

Quellenangaben

[76] EU: siehe Richtlinie 95/46/EG, Artikel 6 Absatz 1 Buchstabe d; WP153, Abschnitt 6.1. Ziffer iii, S. 10; WP108, Abschnitt 8.2.3, S. 8; APEC: siehe Privacy Framework, Part iii, Principle VI, Ziffer 21, S. 20; Program Requirements, Ziffern 21 und 22, S. 15; Intake Questionnaire Frage 22, Frage 23 und Frage 24, S. 13.

[77] EU: siehe Richtlinie 95/46/EG, Artikel 6 Absatz 1 Buchstabe c; WP153, Abschnitt 6.1. Ziffer iii, S. 10; WP108, Abschnitt 8.2.3, S. 8; APEC: siehe Privacy Framework, Part iii, Principle III, Ziffer 18, S. 15, Program Requirements, Frage 6, S. 6.

[78] EU: siehe Richtlinie 95/46/EG, Artikel 6 Absatz 1 Buchstabe d; WP153, Abschnitt 6.1. Ziffer iii,

S. 10.

[79] EU: siehe Richtlinie 95/46/EG, Artikel 6 Absatz 1 Buchstabe e; WP153, Abschnitt 6.1. Ziffer iii, S. 10; WP108, Abschnitt 8.2.3, S. 8.

12. Gründe für die Verarbeitung personenbezogener Daten

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine Selbstverpflichtung enthalten, dass

- personenbezogene Daten nur dann verarbeitet (erhoben, verwendet, übermittelt, offengelegt oder verfügbar gemacht) werden, wenn es einen gültigen Grund für die Verarbeitung gibt, d. h. wenn zum Beispiel die betroffene Person in Kenntnis der Sachlage ihre Zustimmung gegeben hat; [80]
- personenbezogene Daten im Einklang mit den geltenden Rechtsvorschriften verarbeitet werden. [81]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Wenn die Verarbeitung auf der Rechtsgrundlage der Einwilligung erfolgt, dann muss diese eindeutig, konkret und in Kenntnis der Sachlage freiwillig erteilt worden sein. [82] Die Einwilligung als Rechtsgrundlage für die Verarbeitung kann nicht aus Gründen der Offensichtlichkeit oder der öffentlichen Zugänglichkeit der personenbezogenen Daten oder wegen der technischen Undurchführbarkeit der Einwilligung bzw. des Erhalts der personenbezogenen Daten von einem Dritten ersetzt werden. Die Einwilligung ist nur eine der möglichen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Personenbezogene Daten können auch aus folgenden Gründen verarbeitet werden: [83] - Weil die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen, erforderlich ist, oder - weil die Verarbeitung für die Erfüllung	k. A.

einer in der EU geltenden rechtlichen Verpflichtung erforderlich ist, der der für die Verarbeitung Verantwortliche unterliegt, oder - weil die Verarbeitung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist, oder - weil die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt auf EU-Ebene erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde, oder - weil die Verarbeitung zur Verwirklichung des berechtigten Interesses erforderlich ist, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die geschützt sind, überwiegen.	
Klarstellung der Gründe für die Verarbeitung (BCR) k. A.	**Klarstellung der Gründe für die Verarbeitung (CBPR)** Die betroffenen Personen müssen in Bezug auf die Erfassung, Verwendung und Weitergabe ihrer personenbezogenen Daten Wahlmöglichkeiten haben. Bei diesem Grundsatz wird jedoch durch das einleitende „Where appropriate“ (gegebenenfalls) im Privacy Framework selbst der Tatsache Rechnung getragen, dass es Fälle gibt, in denen die Einwilligung offenkundig stillschweigend erteilt worden sein kann oder in denen es nicht notwendig ist, die Ausübung des Wahlrechts zu ermöglichen. Diese Fälle sind unter „Qualifications to the Provision of Choice Mechanisms“ im Einzelnen dargelegt.

	[84] Vorbehaltlich der aufgelisteten Bedingungen muss den betroffenen Personen - die Ausübung ihres Wahlrechts in Bezug auf die Erhebung ihrer personenbezogenen Daten durch leicht erkennbare und verständliche Verfahren ermöglicht werden; - die Ausübung ihres Wahlrechts in Bezug auf die Verwendung ihrer personenbezogenen Daten durch leicht erkennbare und verständliche Verfahren ermöglicht werden; - die Ausübung ihres Wahlrechts in Bezug auf die Weitergabe ihrer personenbezogenen Daten durch leicht erkennbare und verständliche Verfahren ermöglicht werden. - Diese Verfahren müssen eindeutig festgelegt und leicht verständlich, leicht zugänglich und kostengünstig sein. Es kommen unter anderem folgende Bedingungen in Betracht: - Offensichtlichkeit; - Erhebung öffentlich zugänglicher Informationen; - technische Undurchführbarkeit; - Übermittlung durch Dritte; - Weitergabe an eine Regierungsstelle, die mit rechtmäßiger Befugnis um Übermittlung der Daten ersucht hat; - Weitergabe an Dritte im Rahmen eines rechtmäßigen Verfahrens; - rechtmäßige Ermittlungszwecke; - Maßnahmen in Notfallsituationen. Die Verarbeitung personenbezogener Daten kann abgesehen von der Einwilligung aus folgenden Gründen erfolgen: [85]

	- für Zweckbestimmungen, die mit denen vereinbar oder verbunden sind, die in der Datenschutzerklärung oder in der zum Zeitpunkt der Erhebung bereitgestellten Mitteilung angegeben wurden; - weil dies für die Bereitstellung einer von der betroffenen Person bestellten Dienstleistung oder eines entsprechenden Produkts erforderlich ist; - nach Maßgabe der geltenden Gesetze.

Quellenangaben

[80] EU: siehe Richtlinie 95/46/EG, Artikel 7 Buchstabe a; WP154, Abschnitt 5, S. 4; APEC: siehe Privacy Framework, Part iii, Principle III, Ziffer 18, S. 15.

[81] EU: siehe WP153, Abschnitt 6.4, S. 11; WP155, Frage 10, S. 6; APEC: siehe Program Requirements, Frage 7, S. 7.

[82] EU: siehe Richtlinie 95/46/EG, Artikel 7 Buchstabe a; WP154, Abschnitt 5, S. 4.

[83] EU: siehe Richtlinie 95/46/EG, Artikel 7; WP154, Abschnitt 5, p.4.

[84] APEC: siehe Program Requirements Fragen 14-18 und 19, S. 11-14.

[85] APEC: siehe Program Requirements Fragen 8-13, S. 8-10.

13. Sensible Daten

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

In unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen die Schutzmaßnahmen für sensible Daten aufgeführt sein. [86]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen auch eine Selbstverpflichtung dahingehend enthalten, dass die Verarbeitung von sensiblen Daten (z. B. personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Sexualleben und Gesundheit) untersagt ist, ausgenommen in folgenden Fällen: [87] - Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, dieser Einwilligung steht ein gesetzliches Verbot entgegen; oder - die Verarbeitung ist erforderlich, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des EU-Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist; oder - die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben; oder - die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch	Bei der Festlegung der genehmigten Verwendungen von Daten muss die Art der Daten berücksichtigt werden. [89] Die Sicherheitsvorkehrungen müssen der Wahrscheinlichkeit und dem Ausmaß des drohenden Schadens, der Sensibilität der Daten und dem Speicherungskontext angemessen und verhältnismäßig sein. [90]

eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt, im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden; oder - die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat; oder - die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich; oder - die Verarbeitung sensibler Daten ist zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich und erfolgt durch ärztliches Personal, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen. Bei der Verarbeitung sensibler Daten sind erhöhte Sicherheitsmaßnahmen vorzusehen. [88]	

Quellenangaben

[86] EU: siehe Richtlinie 95/46/EG, Artikel 8; WP154, Abschnitt 6, S. 5; APEC: siehe Privacy Framework, Part iii, Principle VII, Ziffer 22, S. 21.

[87] EU: siehe Richtlinie 95/46/EG, Artikel 8; WP154, Ziffer 6, S. 5.

[88] EU: siehe Richtlinie 95/46/EG, Artikel 17 Absatz 1; WP154, Abschnitt 10, S. 7.

[89] APEC: siehe Program Requirements, S. 8.

[90] APEC: siehe Privacy Framework, Part iii, Principle VII, Ziffer 22, S. 21; Program Requirements, Frage 28, Frage 30, Frage 35 a), S. 18-20.

14. Transparenz und Recht auf Information / Informationspflicht

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Allen betroffenen Personen muss vor oder zum Zeitpunkt der Erhebung leichter Zugang zur Datenschutzerklärung gewährt werden. [91] Diese Erklärung muss die nachstehenden Informationen enthalten:

- Angaben darüber, wie die betroffenen Personen über die Übermittlung und Verarbeitung ihrer Personaldaten informiert werden; [92]
- Identität des (der) für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters sowie eine Kontaktstelle; [93]
- Zweckbestimmungen der Verarbeitung der erhobenen Daten; [94]
- weitere Informationen, beispielsweise betreffend
  i. die Empfänger oder Kategorien der Empfänger der Daten; [95]
  ii. das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten sowie Angaben darüber, wie die betroffenen Personen Auskünfte über ihre personenbezogenen Daten erlangen können. [96]

Für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden, besteht unter Umständen keine Pflicht zur Unterrichtung der betroffenen Person. [97] In Bezug auf diese Ausnahmen bestehen Unterschiede zwischen BCR und CBPR. Programmspezifische Anforderungen an BCR und CBPR müssen in den unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre festgelegt sein.

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Den betroffenen Personen sind weitere Angaben bereitzustellen, sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten. [98] Wurden die Daten nicht bei der betroffenen Person erhoben, besteht keine Pflicht zur Unterrichtung der betroffenen Person, wenn die Unterrichtung unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist. [99] Während unter den oben genannten Umständen keine Pflicht zur Unterrichtung der betroffenen Person besteht, wird diese	Die betroffenen Personen müssen von dem Unternehmen auch darüber informiert werden, wie die Daten erhoben werden und auf welchem Wege die Erhebung erfolgt: [100] - direkt von dem Betroffenen oder - durch Dritte im Auftrag des für die Verarbeitung Verantwortlichen oder - auf anderem Wege (muss beschrieben werden). Unter bestimmten Umständen ist eine Unterrichtung unnötig bzw. undurchführbar: [101] - Offensichtlichkeit; - Erhebung öffentlich zugänglicher Informationen;

Pflicht nicht allein aus Gründen der Offensichtlichkeit oder der öffentlichen Zugänglichkeit der verarbeiteten personenbezogenen Daten oder wegen der technischen Undurchführbarkeit der Unterrichtung der betroffenen Person hinfällig noch einzig und allein deshalb, weil die personenbezogenen Daten von einem Dritten übermittelt wurden.	- technische Undurchführbarkeit; - Weitergabe an eine Regierungsstelle, die mit rechtmäßiger Befugnis um Übermittlung der Daten ersucht hat; - Weitergabe an Dritte im Rahmen eines rechtmäßigen Verfahrens; - Übermittlung durch Dritte; - rechtmäßige Ermittlungszwecke; - Maßnahmen in Notfallsituationen. Zusätzliche Informationen, die betroffenen Personen übermittelt werden müssen: - die Tatsache, dass personenbezogene Daten erhoben werden; [102] - die Zwecke, für die die Daten Dritten zugänglich gemacht werden; [103] - Informationen über die Verwendung und Weitergabe von Daten der betroffenen Personen; [104] - die Mittel und Wege, die den betroffenen Personen geboten werden, um die Verwendung und Weitergabe der Daten einzuschränken. [105]

Quellenangaben

[91] EU: siehe Richtlinie 95/46/EG, Artikel 10 und 11; WP153, Abschnitt 1.7, S. 5; WP74, Abschnitt 5.7, S. 19; WP154, Abschnitt 7, S. 5; APEC: siehe Privacy Framework, Part iii, Principle II, Ziffern 15 und 16, S. 12-13 und Ziffer 16, S. 13.

[92] EU: siehe WP74, Abschnitt 5.7, S. 19; WP153, Abschnitt 6.1. Ziffer i, S. 10; APEC: siehe Intake Questionnaire, Frage 1, S. 4; Fragen 17-19, S. 10-11.

[93] EU: siehe WP154, Abschnitt 7, S. 5; APEC: siehe Intake Questionnaire, Frage 1 d), S. 4-5.

[94] EU: siehe WP154, Abschnitt 7, S. 5; APEC: siehe Intake Questionnaire, Frage 1 b) und Frage 3, S. 4-5.

[95] EU: siehe WP154, Abschnitt 7, S. 5; APEC: siehe Privacy Framework, Part iii, Principle II, Ziffer 15 c), S. 12.

[96] EU: siehe WP154, Abschnitt 7, S. 5; APEC: siehe Privacy Framework, Part iii, Principle II, Ziffer 15 e), S. 12; Intake Questionnaire, Frage 38 a), S. 18.

[97] EU: siehe Richtlinie 95/46/EG, Artikel 10 und 11; APEC: siehe Intake Questionnaire, Qualifications to the Provision of Notice, S. 6.

[98] EU: siehe Richtlinie 95/46/EG, Artikel 10.

[99] EU: siehe Richtlinie 95/46/EG, Artikel 11.

[100] APEC: siehe Intake Questionnaire, Frage 1 a), S. 4 und Frage 5, S. 7.

[101] APEC: siehe Intake Questionnaire, Qualifications to the Provision of Notice, S. 6.

[102] APEC: siehe Privacy Framework, Part iii, Principle II, Ziffer 15 a), S. 12.

[103] APEC: siehe Intake Questionnaire, Frage 1 c), S. 4.

[104] APEC: siehe Intake Questionnaire, Frage 1 e), S. 5.

[105] APEC: siehe Privacy Framework, Part iii, Principle II, Ziffer 15 e), S. 12; Intake Questionnaire, Fragen 15-16, S. 10.

15. Recht auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten/Zugang und Korrektur

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Es muss sichergestellt werden, dass [106]

- alle betroffenen Personen die Möglichkeit haben, von dem für die Verarbeitung Verantwortlichen Auskunft darüber zu erhalten, ob dieser im Besitz sie betreffender personenbezogener Daten ist; [107]
- alle betroffenen Personen die Möglichkeit haben, eine Kopie aller Daten zu erhalten, die sich im Besitz des Unternehmens befinden. Die betreffenden Daten müssen ohne Einschränkung innerhalb einer angemessenen Zeit und zu einer angemessenen Gebühr (bzw. kostenlos) zur Verfügung gestellt werden; [108]
- alle betroffenen Personen die Möglichkeit haben, von dem für die Verarbeitung Verantwortlichen die Berichtigung oder Löschung von Daten zu verlangen, insbesondere wenn diese Daten unvollständig oder unrichtig sind. [109]

Diese Verpflichtungen unterliegen Ausnahmen und Voraussetzungen gemäß den anwendbaren Rechtsvorschriften. [110]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Bei den oben genannten Elementen handelt es sich um Rechte, die den betroffenen Personen zustehen. Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen auch sicherstellen, dass alle betroffenen Personen das Recht haben, von einem für die Verarbeitung Verantwortlichen die Sperrung von Daten zu verlangen, insbesondere wenn die Daten unvollständig oder unrichtig sind. [111]	Die für die Verarbeitung Verantwortlichen müssen Maßnahmen zur Bestätigung der Identität der betroffenen Person treffen, die um Zugang ersucht. [112] Die Bereitstellung von Daten an eine betroffene Person, die ihr Recht auf Zugriff ausübt, muss angemessen und allgemeinverständlich und in einer Form erfolgen, die der üblichen Interaktion mit der betreffenden Person entspricht. [113] Es besteht die Verpflichtung, Berichtigungen oder Löschung innerhalb einer angemessenen Frist vorzunehmen. [114] Die für die Verarbeitung Verantwortlichen übermitteln den betroffenen Personen eine Kopie der berichtigten personenbezogenen Daten oder eine Bestätigung, dass die Daten berichtigt oder gelöscht wurden. [115] Die für die Verarbeitung Verantwortlichen übermitteln den betroffenen Personen eine

	Erklärung dafür, warum kein Zugang zu den Daten gewährt wird bzw. warum diese nicht berichtigt werden, sowie Kontaktinformationen für weitergehende Nachfragen zur Verweigerung des Zugangs oder der Berichtigung. [116]
Ausnahmen von den Zugangsrechten (BCR) Die Rechtsvorschriften der EU-Mitgliedstaaten zum Datenschutz können Ausnahmen vom Zugangsrecht der betroffenen Personen vorsehen, die auf den Rechtsvorschriften der EU-Mitgliedstaaten beruhen und eng auszulegen sind, sodass sich Unternehmen gezwungen sehen können, Zugangsersuchen abzulehnen, sofern dies notwendig ist für [117] a) die Sicherheit des Staates; b) die Landesverteidigung; c) die öffentliche Sicherheit; d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen; e) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten; f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind; g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen. Die Rechtsvorschriften der EU-Mitgliedstaaten zum Datenschutz können	**Ausnahmen von den Zugangsrechten (CBPR)** Unter bestimmten Umständen kann es notwendig sein, Zugangsersuchen aus folgenden Gründen abzulehnen: [118] - übermäßige Belastungen; - Schutz vertraulicher Informationen; - Haftpflichtrisiko.

vorsehen, dass vorbehaltlich angemessener rechtlicher Garantien, mit denen insbesondere ausgeschlossen wird, dass die Daten für Maßnahmen oder Entscheidungen gegenüber bestimmten Personen verwendet werden, die Zugangsrechte der betroffenen Personen in Fällen, in denen offensichtlich keine Gefahr eines Eingriffs in die Privatsphäre der betroffenen Person besteht, eingeschränkt werden, wenn die Daten ausschließlich für Zwecke der wissenschaftlichen Forschung verarbeitet werden oder personenbezogen nicht länger als erforderlich lediglich zur Erstellung von Statistiken aufbewahrt werden.	

Quellenangaben

[106] EU: siehe Richtlinie 95/46/EG, Artikel 12; WP153, Abschnitt 6.1. Ziffer v), S. 10; WP108, Abschnitt 8.2.5, S. 8.

[107] APEC: siehe Privacy Framework, Part iii, Principle VIII, Ziffer 23 a), S. 22; Intake Questionnaire, Frage 36, S. 17.

[108] APEC: siehe Privacy Framework, Part iii, Principle VIII, Ziffer 23 b), S. 22, Intake Questionnaire, Fragen 37, 37 b) und 37 e), S. 17-18.

[109] APEC: siehe Privacy Framework, Part iii, Principle VIII, Ziffer 23 c), S. 22; Intake Questionnaire, Fragen 38 und 38 b), S. 18-19.

[110] EU: siehe Richtlinie 95/46/EG, Artikel 13; APEC: siehe Intake Questionnaire, Qualifications to the Provision of Access and Correction Mechanisms, S. 19-20.

[111] EU: siehe Richtlinie 95/46/EG, Artikel 12.

[112] APEC: siehe Intake Questionnaire, Frage 37 a), S. 17.

[113] APEC: siehe Intake Questionnaire, Fragen 37 c) und d), S. 18.

[114] APEC: siehe Intake Questionnaire, Frage 38 a), S. 19.

[115] APEC: siehe Intake Questionnaire, Frage 38 d), S. 19.

[116] APEC: siehe Privacy Framework, Part iii, Principle VIII, Ziffer 25, S. 24, Intake Questionnaire, Frage 38 e), S. 19.

[117] EU: siehe Richtlinie 95/46/EG, Artikel 13.

[118] APEC: siehe Intake Questionnaire, Qualifications to the Provision of Access and Correction Mechanisms, S. 19-20.

16. Widerspruchsrecht / Wahlmöglichkeit

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Gegebenenfalls bzw. nach Maßgabe des anwendbaren Rechts muss sichergestellt werden, dass die betroffene Person gemäß den geltenden Rechtsvorschriften Widerspruch gegen die Verarbeitung ihrer Daten einlegen bzw. sich gegen die Verarbeitung ihrer personenbezogenen Daten entscheiden kann. [119]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen auch sicherstellen, dass jede betroffene Person das Recht hat, Widerspruch gegen die Verarbeitung ihrer personenbezogenen einzulegen, da den betroffenen Personen ein solches Recht zusteht. Das Widerspruchsrecht kann von den betroffenen Personen jederzeit ausgeübt werden. Insbesondere hat jede betroffene Person das Recht, auf Antrag kostenfrei gegen eine vom für die Verarbeitung Verantwortlichen beabsichtigte Verarbeitung sie betreffender personenbezogener Daten für Zwecke der Direktwerbung Widerspruch einzulegen und vor der ersten Weitergabe personenbezogener Daten an Dritte oder vor deren erstmaliger Nutzung im Auftrag Dritter zu Zwecken der Direktwerbung informiert und ausdrücklich auf das Recht hingewiesen zu werden, kostenfrei gegen eine solche Weitergabe oder Nutzung Widerspruch einzulegen.	k. A.
Ausnahmen vom Widerspruchsrecht (BCR)	**Ausnahmen von der Wahlmöglichkeit (CBPR)**
k. A.	Unter bestimmten Umständen ist es unnötig oder undurchführbar, den betroffenen Personen Wahlmöglichkeiten einzuräumen: [120]

	- Offensichtlichkeit; - Erhebung öffentlich zugänglicher Informationen; - technische Undurchführbarkeit; - Übermittlung durch Dritte; - Weitergabe an eine Regierungsstelle, die mit rechtmäßiger Befugnis um Übermittlung der Daten ersucht hat; - Weitergabe an Dritte im Rahmen eines rechtmäßigen Verfahrens; - rechtmäßige Ermittlungszwecke; - Maßnahmen in Notfallsituationen.
Klarstellung des Widerspruchsrechts (BCR) Betroffene Personen haben jederzeit das Recht, ihre Einwilligung zurückzuziehen. Darüber hinaus können sie auch dann Widerspruch einlegen, wenn die Verarbeitung auf der Basis einer anderen Rechtsgrundlage erfolgt. Ferner ist in den Rechtsvorschriften der EU-Mitgliedstaaten zum Datenschutz festgelegt, unter welchen Umständen betroffene Personen - zumindest wenn die Rechtsgrundlage für die Verarbeitung von Artikel 7 Buchstabe e der Richtlinie 95/46/EG abgeleitet ist - aus zwingenden, schutzwürdigen Gründen, die sich aus ihrer persönlichen Situation ergeben, Widerspruch einlegen können; dies gilt nicht bei einer im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung. Im Fall eines berechtigten Widerspruchs kann sich die vom für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung nicht mehr auf diese Daten beziehen. [121] Das Widerspruchsrecht kann nicht aus Gründen der Offensichtlichkeit oder der öffentlichen Zugänglichkeit der verarbeiteten	**Klarstellung der Wahlmöglichkeit (CBPR)** Die Unternehmen müssen den betroffenen Personen Wahlmöglichkeiten in Bezug auf die Erfassung, Verwendung und Weitergabe ihrer personenbezogenen Daten bieten. [122]

personenbezogenen Daten oder wegen der technischen Undurchführbarkeit des Widerspruchsrechts bzw. des Erhalts der personenbezogenen Daten von einem Dritten hinfällig werden.	

Quellenangaben

[119] EU: siehe Richtlinie 95/46/EG, Artikel 14, WP153, Abschnitt 6.1. Ziffer v, S. 10; WP108, Abschnitt 8.2.5, S. 8; APEC: siehe Intake Questionnaire, Fragen 14-16.

[120] APEC: siehe Intake Questionnaire, Qualifications to the Provision of Choice Mechanisms, S. 11-12.

[121] EU: siehe Richtlinie 95/46/EG, Artikel 14.

[122] APEC: siehe Program Requirements, Fragen 14 bis 16, S. 11-13.

17. Automatisierte Einzelentscheidungen

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

k. A.

Für die Genehmigung von BCR erforderliche Elemente	**Für die Zertifizierung von CBPR erforderliche Elemente**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine Selbstverpflichtung enthalten, dass keine Entscheidung, die die betroffene Person erheblich beeinträchtigt, ausschließlich auf eine automatisierte Verarbeitung ihrer Daten gestützt wird, es sei denn [123] - die Entscheidung ergeht im Rahmen des Abschlusses oder der Erfüllung eines Vertrags und dem Ersuchen der betroffenen Person auf Abschluss oder Erfüllung des Vertrags wurde stattgegeben oder die Wahrung ihrer berechtigten Interessen wird durch geeignete Maßnahmen ‑ beispielsweise die Möglichkeit, ihren Standpunkt geltend zu machen ‑ garantiert; oder - ist durch ein Gesetz zugelassen, das auch Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt.	k. A.

Quellenangaben

[123] EU: siehe WP154, Abschnitt 9, S. 6.

18. Sicherheit und Vertraulichkeit

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine Selbstverpflichtung zur Anwendung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen enthalten, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe bzw. dem unberechtigten Zugang und allen anderen Formen der unberechtigten Verarbeitung schützen. [124]

Diese Maßnahmen müssen ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. [125]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen darüber hinaus die Anforderung enthalten, dass Sicherheitsmaßnahmen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten umgesetzt werden müssen. [126]	Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen darüber hinaus die Anforderung enthalten, dass die Sicherheitsvorkehrungen einer regelmäßigen Überprüfung und Neubewertung unterzogen werden. [127] Es müssen Maßnahmen für die Informationssicherheit [128] und die sichere Vernichtung [129] personenbezogener Daten umgesetzt werden. Ferner müssen Vorkehrungen zur Erkennung und Verhinderung von Angriffen, des Eindringens in Datenbestände oder sonstiger Sicherheitsprobleme und zur Reaktion darauf getroffen werden. [130] Die Mitarbeiter müssen nachweislich durch regelmäßige Schulungen und Anleitungen dafür sensibilisiert werden, wie wichtig es ist, die Sicherheit personenbezogener Daten zu achten und aufrechtzuerhalten, und welche Verpflichtungen in diesem Zusammenhang bestehen. [131]

Quellenangaben

[124] EU: siehe Richtlinie 95/46/EG, Artikel 17 Absatz 1; WP108, Abschnitt 8.2.4, S. 8; APEC: siehe Privacy Framework, Part iii, Principle VII, Ziffer 22, S. 2; Intake Questionnaire, Frage 27, S. 14.

[125] EU: siehe Richtlinie 95/46/EG, Artikel 17 Absatz 1; APEC: siehe Privacy Framework, Part iii, Principle VII, Ziffer 22, S. 21, Intake Questionnaire, Frage 28, S. 14.

[126] EU: siehe Richtlinie 95/46/EG, Artikel 17 Absatz 1.

[127] APEC: siehe Privacy Framework, Part iii, Principle VII, Ziffer 22, S. 21.

[128] APEC: siehe Intake Questionnaire, Frage 26, S. 14.

[129] APEC: siehe Intake Questionnaire, Frage 31, S. 15.

[130] APEC: siehe Intake Questionnaire, Frage 32 und 33, S. 15.

[131] APEC: siehe Intake Questionnaire, Fragen 29 und 30 a), S. 14.

19. Schulungsprogramm

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen geeignete Schulungen der Mitarbeiter über die einschlägigen Regelungen vorsehen. [132]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die Anforderung in Bezug auf die Durchführung von Schulungen betrifft Mitarbeiter, die ständigen oder regelmäßigen Zugang zu Personaldaten haben, die solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln. [133]	Die Schulungen müssen Datenschutzgrundsätze und -verfahren sowie das Vorgehen bei Beschwerden im Zusammenhang mit dem Datenschutz umfassen. [134] Die Mitarbeiter müssen nachweislich durch regelmäßige Schulungen und Anleitungen dafür sensibilisiert werden, wie wichtig es ist, die Sicherheit personenbezogener Daten zu achten und aufrechtzuerhalten, und welche Verpflichtungen in diesem Zusammenhang bestehen. [135]

Quellenangaben

[132] EU: siehe WP74, Abschnitt 5.1, S. 16; APEC: siehe Intake Questionnaire, Frage 44, S. 22.

[133] EU: siehe WP153, Abschnitt 2.1, S. 5.

[134] APEC: siehe Program requirements, Frage 44, S. 25-26.

[135] APEC: siehe Intake Questionnaire, Frage 30 a), S. 14.

20. Überwachungs- und Auditprogramm

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen die Überwachung der Anwendung und der Einhaltung der betreffenden Regelungen vorsehen. [136]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen auch die Selbstverpflichtung enthalten, die Einhaltung der betreffenden Regelungen innerhalb der Unternehmensgruppe einem Audit zu unterziehen, das sich insbesondere auf Folgendes erstreckt: [137] - Das Auditprogramm erstreckt sich auf alle Aspekte der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre und sieht Verfahren vor, mit denen sichergestellt wird, dass Abhilfemaßnahmen getroffen werden. - Datenschutzaudits müssen regelmäßig (zeitliche Vorgabe) durch interne oder externe akkreditierte Auditoren oder auf Antrag des Datenschutzbeauftragten (oder einer anderen zuständigen Stelle im Unternehmen) durchgeführt werden. - Die Auditergebnisse werden dem Datenschutzbeauftragten (oder einer anderen zuständigen Stelle im Unternehmen) und der Unternehmensleitung mitgeteilt. - Die Datenschutzbehörden in der EU können eine Kopie dieser Audits anfordern. - Im Auditplan ist vorzusehen, dass die Datenschutzbehörden in der EU bei Bedarf ein eigenes Datenschutzaudit	Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen auch die Anforderung enthalten, dass der für die Verarbeitung Verantwortliche jährlich die fortgesetzte Einhaltung der Anforderungen des CBPR-Programms nachweist. [138] Die APEC Accountability Agents führen regelmäßig umfassende Überprüfungen durch, um die Richtigkeit der erneuten Zertifizierung sicherzustellen. [139] Um die Einhaltung seiner Weisungen und/oder der Vereinbarungen/Verträge sicherzustellen, kontrolliert und überwacht der für die Verarbeitung Verantwortliche regelmäßig und stichprobenartig die Verarbeiter, Agenten, Auftragnehmer oder sonstigen Dienstleister, die von ihm mit der Verarbeitung personenbezogener Daten beauftragt wurden. [140]

durchführen können. - Jedes Mitglied der Unternehmensgruppe muss solche Prüfungen der Datenschutzbehörden in der EU dulden und deren Mitteilungen, die die Anwendung der BCR betreffen, nachkommen.	

Quellenangaben

[136] EU: siehe WP74, Abschnitt 5.2, S. 16; APEC: siehe Recognition application, Annex A, Ziffern 6-8, S. 6.

[137] EU: siehe WP153, Abschnitt 2.3, S. 7.

[138] APEC: siehe Recognition application, Annex A, Ziffer 8, S. 6.

[139] APEC: siehe Recognition application, Annex A, Ziffer 8, S. 6.

[140] APEC: siehe Intake Questionnaire, Frage 49, S. 23.

21. Einhaltung und Überwachung

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen die Ernennung eines geeigneten Stabs (z. B. eines Stabs von Datenschutzbeauftragten) für die Aufsicht und Sicherstellung der Einhaltung der betreffenden Regelungen vorsehen. [141]

Zusätzliche Elemente für die BCR-Genehmigung [142]	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Darüber hinaus müssen die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre eine kurze Beschreibung der Struktur, Aufgaben und Zuständigkeiten der Mitarbeiter/Datenschutzbeauftragten o. ä. enthalten, die die Einhaltung der betreffenden Regelungen gewährleisten sollen. Die mit dieser Aufgabe betrauten Mitarbeiter werden von der obersten Leitungsebene unterstützt. Beispiel für die Struktur, Aufgaben und Zuständigkeiten des Stabs der Mitarbeiter/Datenschutzbeauftragten o. ä., der die Einhaltung der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre gewährleisten soll: Der oberste Datenschutzbeauftragte berät die Unternehmensleitung, ist zuständig bei Untersuchungen der nationalen Datenschutzbehörden in der EU, berichtet jährlich über die Anwendung der BCR, sorgt auf Unternehmensebene für die Einhaltung der BCR; die Datenschutzbeauftragten bearbeiten die Beschwerden der Betroffenen in ihrem Zuständigkeitsbereich, berichten dem obersten Datenschutzbeauftragten über größere Probleme beim Datenschutz und sorgen für die Einhaltung der Vorschriften auf lokaler Ebene.	Darüber hinaus müssen die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre eine Anforderung enthalten, nach der die ernannte(n) Person(en) geeignete Verfahren für die Entgegennahme, Prüfung und Beantwortung von Beschwerden im Zusammenhang mit dem Datenschutz umsetzen und gegebenenfalls eine Begründung zu eventuellen Abhilfemaßnahmen vorlegen müssen. [143]

Quellenangaben

[141] EU: siehe WP74, Abschnitt 5.1, S. 16; APEC: siehe Intake Questionnaire, Frage 40, S. 21.

[142] EU: siehe WP153, Abschnitt 2.4, S. 8.

[143] APEC: siehe Program requirements, Frage 40, S. 24-25.

22. Interne Beschwerdeverfahren

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen ein Beschwerdeverfahren vorsehen, das folgenden Grundsätzen genügt: [144]

- Jede betroffene Person muss Beschwerde mit der Begründung erheben können, dass ein Mitglied der Unternehmensgruppe gegen die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre verstößt.
- Mit den Beschwerden muss sich eine klar bezeichnete Beschwerdeabteilung oder Person befassen.

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die benannte Abteilung/Person, die sich mit den Beschwerden befasst, muss bei der Wahrnehmung dieser Aufgabe über ein entsprechendes Maß an Unabhängigkeit verfügen. [145]	Die Antwort auf Beschwerden von betroffenen Personen muss eine Begründung zu den Abhilfemaßnahmen enthalten, die auf die entsprechende Beschwerde hin ergriffen wurden. [146]

Quellenangaben

[144] EU: siehe WP74, Abschnitt 5.3, S. 17; APEC: siehe Intake Questionnaire, Fragen 41-42, S. 21.

[145] EU: siehe WP74, Abschnitt 5.3, S. 17.

[146] APEC: siehe Intake Questionnaire, Frage 43, S. 21.

23. Aktualisierung der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen vorsehen, dass alle signifikanten Änderungen der betreffenden Regelungen oder der Mitgliederliste allen Mitgliedern der Unternehmensgruppe sowie den Datenschutzbehörden in der EU und den APEC Accountability Agents mitgeteilt werden, um Änderungen des rechtlichen Umfelds oder der Unternehmensstruktur sowie insbesondere der Tatsache Rechnung zu tragen, dass einige Änderungen möglicherweise von den nationalen Datenschutzbehörden in der EU erneut genehmigt und/oder von den APEC Accountability Agents überprüft werden müssen. [147]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen darüber hinaus eine Selbstverpflichtung dahingehend enthalten, dass substanzielle Änderungen der betreffenden Regelungen auch den betroffenen Personen mitgeteilt werden. [148] Die Aktualisierung der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre oder der Liste der Mitglieder der Unternehmensgruppe, die an die betreffenden Regelungen gebunden sind, ist unter folgenden Voraussetzungen möglich, ohne eine neue Genehmigung beantragen zu müssen: [149] i) Es wird eine Person benannt, die eine stets aktualisierte Liste der Gruppenmitglieder führt, Änderungen der Regelungen für den Schutz personenbezogener Daten und der Privatsphäre erfasst und den betroffenen Personen oder Datenschutzbehörden in der EU auf Anfrage diesbezügliche Auskünfte erteilt. ii) Einem neuen Mitglied der Unternehmensgruppe dürfen	Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen darüber hinaus eine Anforderung dahingehend enthalten, dass bei wesentlichen Änderungen der betreffenden Regelungen (die vom APEC Accountability Agent nach Treu und Glauben festgestellt wurden), eine sofortige Überprüfung durch den Accountability Agent durchgeführt wird. [150] Die Unternehmen sollten eine aktuelle Erklärung zu ihren Verfahren und Grundsätzen in Bezug auf personenbezogene Daten vorlegen. [151] Darüber hinaus müssen die Unternehmen den betroffenen Personen Wahlmöglichkeiten in Bezug auf die Erfassung, Verwendung und Weitergabe ihrer personenbezogenen Daten bieten. [152]

	personenbezogene Daten erst dann übermittelt werden, wenn die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre für dieses neue Mitglied gelten und die Einhaltung der Vorschriften gewährleistet ist. iii) Änderungen der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre oder der Mitgliederliste sollten den nationalen Datenschutzbehörden in der EU jährlich mit einer kurzen Begründung der Änderungen gemeldet werden.	

Quellenangaben

[147] EU: siehe WP74, Abschnitt 4.2, S. 15; APEC: siehe Recognition application, Annex A, Ziffer 8, S. 6.

[148] EU: siehe WP154, Abschnitt 21, S. 9-10.

[149] EU: siehe WP74, Abschnitt 4.2, S. 15.

[150] APEC: siehe Recognition application, Annex A, Ziffer 8, S. 6.

[151] APEC: siehe Privacy Framework, Part iii, Principle II, Ziffer 15; Intake Questionnaire, Frage 1, S. 4.

[152] APEC: siehe Program Requirements, Fragen 14 bis 16, S. 11-13.

24. Vorgehen bei einzelstaatlichen Rechtsvorschriften, die der Einhaltung der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre entgegenstehen können, und bei Auskunftsbegehren von Strafverfolgungsbehörden

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

k. A.

Für die Genehmigung von BCR erforderliche Elemente [153]	**Für die Zertifizierung von CBPR erforderliche Elemente**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine eindeutige Bestimmung enthalten, nach der ein Mitglied der Unternehmensgruppe, das Anlass zu der Annahme hat, dass die geltenden Rechtsvorschriften es daran hindern, seinen Verpflichtungen im Rahmen der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre nachzukommen, und dass diese Rechtsvorschriften die durch diese Regelungen gebotenen Garantien wesentlich beeinträchtigen, die Hauptniederlassung der Unternehmensgruppe in der EU oder das Unternehmen, das in der EU die Haftung für den Datenschutz übernommen hat, oder den zuständigen Datenschutzbeauftragten unverzüglich informieren muss (sofern dem nicht ein Verbot einer Strafverfolgungsbehörde entgegensteht, z. B. zur Wahrung des Untersuchungsgeheimnisses in einer Strafsache). Darüber hinaus müssen die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre vorsehen, dass im Falle einer Kollision zwischen nationalem Recht und den Verpflichtungen, Anforderungen und Zusicherungen, die in den betreffenden Regelungen enthalten sind, die EU-Hauptniederlassung, das Unternehmen, das in	Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen eine Anforderung enthalten, nach der es ein Verfahren für den Fall von gerichtlichen oder anderen amtlichen Vorladungen, Verfügungen oder Anordnungen einschließlich derjenigen geben muss, in denen die Offenlegung personenbezogener Daten verlangt wird. [154]

der EU die Haftung für den Datenschutz übernommen hat, oder der zuständige Datenschutzbeauftragte die zuständigen nationalen Datenschutzbehörden in der EU konsultiert und eine verantwortungsvolle Entscheidung über das weitere Vorgehen trifft. Alle diesen Abschnitt der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre betreffenden Vorfälle werden im Rahmen der in Abschnitt 20 vorgesehenen regelmäßigen Audits erfasst und überprüft.	

Quellenangaben

[153] EU: siehe WP74, Abschnitt 3.3.3, S. 13-14 und WP154, Abschnitt 16, S. 8.

[154] APEC: siehe Intake Questionnaire, Frage 45, S. 22.

25. Gegenseitige Unterstützung und Zusammenarbeit mit den nationalen Datenschutzbehörden in der EU / den Datenschutzbehörden (Privacy Enforcement Authorities, PEA) der APEC

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

k. A.

Für die Genehmigung von BCR erforderliche Elemente	**Für die Zertifizierung von CBPR erforderliche Elemente**
Die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre müssen vorsehen, dass [155] - die Mitglieder der Unternehmensgruppe verpflichtet sind, bei der Bearbeitung eines Antrags oder einer Beschwerde von einer betroffenen Person oder bei einer Untersuchung oder Ermittlung durch Datenschutzbehörden in der EU zusammenzuarbeiten und sich gegenseitig zu unterstützen. - die Unternehmensteile verpflichtet sind, sich an die Empfehlungen der nationalen Datenschutzbehörden in der EU zu Fragen der Auslegung der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre zu halten.	Unternehmen aus den teilnehmenden Ländern können eine Zertifizierung der CBPR erhalten. APEC-Länder können am CBPR-System nur teilnehmen, wenn ihre Datenschutzbehörde (PEA) dem APEC-Abkommen über die grenzüberschreitende Durchsetzung des Datenschutzes (CPEA) angehört. [156]

Quellenangaben

[155] EU: siehe WP74, Abschnitt 5.4, S. 17.

[156] APEC: siehe JOP Charter, Abschnitt 2.2 Ziffer i, S. 15.

26. Verhältnis zwischen dem einzelstaatlichen Recht und den unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

k. A.

Für die Genehmigung von BCR erforderliche Elemente	**Für die Zertifizierung von CBPR erforderliche Elemente**
Werden personenbezogene Daten in der EU verarbeitet, so sind die EU-Datenschutzvorschriften anzuwenden. Daher muss in den unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre festgelegt werden, dass [157] - in Fällen, in denen das einzelstaatliche Recht ein höheres Schutzniveau für personenbezogene Daten vorschreibt, dieses Recht den unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre vorgeht; - die Datenverarbeitung in jedem Fall nach Maßgabe des Rechts des betreffenden Mitgliedstaats im Sinne von Artikel 4 der Richtlinie 95/46/EG erfolgt.	k. A.
Klarstellung des Verhältnisses zwischen dem einzelstaatlichen Recht und BCR k. A.	**Klarstellung des Verhältnisses zwischen dem einzelstaatlichen Recht und CBPR** [158] Die Teilnahme am CBPR-System ersetzt nicht die Pflichten des teilnehmenden Unternehmens gemäß den einzelstaatlichen Rechtsvorschriften. Gibt es in einem Land keine anwendbaren einzelstaatlichen Datenschutzanforderungen, so sollen die unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der

	Privatsphäre ein Mindestschutzniveau gewährleisten. Einzelstaatliche Rechtsvorschriften und Regelungen, die über das hinausgehen, was im Rahmen der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre vorgesehen ist, gelten weiterhin uneingeschränkt. Gehen die Anforderungen der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre über die Anforderungen der einzelstaatlichen Rechtsvorschriften und Regelungen hinaus, so muss das betreffende Unternehmen diese zusätzlichen Anforderungen als Voraussetzung für seine Teilnahme erfüllen. Die Datenschutzbehörden des betreffenden Landes sollten jedoch in der Lage sein, im Rahmen der geltenden innerstaatlichen Rechtsvorschriften und Regelungen Durchsetzungsmaßnahmen zum Schutz personenbezogener Informationen zu treffen, die mit den Anforderungen des CBPR-Programms im Einklang stehen.

Quellenangaben

[157] EU: siehe WP74, Abschnitt 3.3.3, S. 13-14.

[158] APEC: siehe Policies, Rules and Guidelines, Ziffern 43 und 44, S. 10-11.

27. Schlussbestimmungen

Übereinstimmende Elemente, die sowohl für die BCR-Genehmigung als auch für die CBPR-Zertifizierung erforderlich sind

In unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre ist der Zeitpunkt des Inkrafttretens anzugeben. [159]

Quellenangaben

[159] EU: siehe WP154, Abschnitt 23, S. 10; APEC: siehe Program requirements, Frage 1, S. 2.

Brüssel, den 27. Februar 2014

Für die Arbeitsgruppe
Der Vorsitzende
Jacob KOHNSTAMM

Anhänge

Anhang 1. Unterlagen, die von den Unternehmen zur Beantragung der BCR-Genehmigung durch die nationalen Datenschutzbehörden in der EU bzw. zur Beantragung der CBPR-Zertifizierung durch die APEC Accountability Agents einzureichen sind

Anhang 1. Unterlagen, die von den Unternehmen zur Beantragung der BCR-Genehmigung durch die nationalen Datenschutzbehörden in der EU bzw. zur Beantragung der CBPR-Zertifizierung durch die APEC Accountability Agents einzureichen sind

Ein Unternehmen, das die Genehmigung der BCR bzw. die Zertifizierung der CBPR beantragt, muss den nationalen Datenschutzbehörden in der EU bzw. im Falle der APEC dem Accountability Agent sämtliche Unterlagen vorlegen, die Aufschluss über die Einhaltung der in den unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre verankerten Verpflichtungen, Anforderungen und Zusicherungen geben, z. B.: [160]

- Unterlagen, die Aufschluss über die Datenschutzpolitik u. a. gegenüber Kunden oder Mitarbeitern geben, und aus denen hervorgeht, wie die Betroffenen über den Schutz ihrer personenbezogenen Daten in der Unternehmensgruppe informiert werden; [161]

- Leitlinien für die Beschäftigten, die Zugang zu personenbezogenen Daten haben, um ihnen das Verständnis und die Anwendung der Datenschutzregelungen zu erleichtern (z. B. Leitlinien für den Umgang mit Beschwerden von betroffenen Personen, für die Information der betroffenen Personen, für geeignete Maßnahmen zur Gewährleistung der Sicherheit/Vertraulichkeit der Datenverarbeitung); [162]

- Beschreibung des Schulungsprogramms und/oder Beispiele; [163]

- Beschreibung des internen Beschwerdeverfahrens; [164]

- Sicherheitspolitik in Bezug auf IT-Systeme, mit denen personenbezogene Daten aus der EU bzw. der APEC verarbeitet werden; [165]

- Musterverträge für Datenverarbeiter (innerhalb oder außerhalb der Unternehmensgruppe), die personenbezogene Daten aus der EU bzw. aus der APEC verarbeiten. [166]

Zusätzliche Elemente für die BCR-Genehmigung	**Zusätzliche Elemente für die CBPR-Zertifizierung**
Darüber hinaus muss das antragstellende Unternehmen bei den nationalen Datenschutzbehörden in der EU folgende Unterlagen einreichen: - Stellenbeschreibung des Datenschutzbeauftragten oder anderer Personen, die für den Datenschutz in der Unternehmensgruppe zuständig sind; - Antragsformular WP133; [167]	Darüber hinaus muss das antragstellende Unternehmen bei den APEC Accountability Agents folgende Unterlagen einreichen: - Intake Questionnaire (Aufnahmefragebogen), - Beispiele für zusätzliche Unterlagen, die APEC Accountability Agents möglicherweise für die Überprüfung der unternehmensinternen Regelungen für

- Datenschutzauditplan und –programm unter Angabe der zuständigen Personen (interne/externe akkreditierte Auditoren der Unternehmensgruppe); - Nachweis, dass das Unternehmen, von dem aus die Daten aus der EU in Drittländer übermittelt werden, und entweder die EU-Hauptniederlassung oder das in der EU haftende Unternehmen über ausreichende Mittel verfügen, um den Schaden zu ersetzen, der aus einer Verletzung der unternehmensinternen Regelungen für den Schutz personenbezogener Daten und der Privatsphäre entstanden ist.	den Schutz personenbezogener Daten und der Privatsphäre benötigen: - Beispiele für Mitteilungen an betroffene Personen; [168] - Unterlagen, die die Einhaltung der Beschränkungen der Datenerhebung belegen, mit folgenden Angaben: [169] i) alle Arten von Daten, die erhoben werden, ii) erklärter Zweck der Erhebung der einzelnen Datenarten und iii) alle Verwendungen der einzelnen Datenarten, iv) Erläuterung der Vereinbarkeit oder des Zusammenhangs der genannten Verwendungen mit dem erklärten Zweck der Erhebung; - Unterlagen, die belegen, dass die personenbezogenen Daten nur zu den erklärten Zwecken oder anderen damit vereinbaren oder zusammenhängenden Zwecken erhoben, verwendet und weitergegeben werden, sofern Anderes nicht unter bestimmten Umständen zulässig ist; [170] - Unterlagen, aus denen hervorgeht, welche Möglichkeiten den betroffenen Personen zur Ausübung ihres Wahlrechts in Bezug auf die Erhebung, Verwendung und Weitergabe ihrer personenbezogenen Daten zur Verfügung gestellt werden, und die belegen, dass die betreffenden Wahlmöglichkeiten bestehen und anwendungsfähig sind und der Zweck der Erhebung klar und deutlich angegeben ist; [171] - Verfahren, die eingeführt wurden, um zu überprüfen und zu gewährleisten, dass die personenbezogenen Daten entsprechend den Erfordernissen des Verwendungszwecks aktuell, richtig und

	vollständig sind; [172] - Nachweise für das Vorliegen von Vereinbarungen mit Verarbeitern, Agenten, Auftragnehmern oder sonstigen Dienstleistern, um zu gewährleisten, dass die Verpflichtungen des für die Verarbeitung Verantwortlichen gegenüber den betroffenen Personen eingehalten werden. [173]

Quellenangaben

[160] EU: siehe WP154, Bei den Datenschutzbehörden einzureichende Unterlagen, S. 10-11.

[161] APEC: siehe Program requirements, Frage 1, S. 2-4.

[162] APEC: siehe Program requirements, Frage 29, S. 18; Frage 44, S. 25-26.

[163] APEC: siehe Program requirements, Frage 44, S. 25-26.

[164] APEC: siehe Program requirements, Fragen 41-43, S. 25.

[165] APEC: siehe Program requirements, Frage 26, S. 17; Frage 31, S. 19.

[166] APEC: siehe Program requirements, Frage 46, S. 26-27.

[167] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp133_en.doc.

[168] APEC: siehe Program requirements, Frage 2, S. 4.

[169] APEC: siehe Program requirements, Frage 6, S. 6.

[170] APEC: siehe Program requirements, Frage 8, S. 8.

[171] APEC: siehe Program requirements, Fragen 14-17, S. 11-13.

[172] APEC: siehe Program requirements, Frage 21, S. 15.