1271-00-01/08/DE
WP 154

Arbeitsdokument „Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)“

Angenommen am 24. Juni 2008

EINFÜHRUNG

Innerhalb einer Unternehmensgruppe dürfen personenbezogene Daten auf der Grundlage verbindlicher unternehmensinterner Datenschutzregelungen (Binding Corporate Rules – BCR) aus der EU in Drittländer übermittelt werden. Die Datenschutzgruppe hat in ihren Arbeitsdokumenten WP 74[1] und WP 108[2] Überlegungen zu den wesentlichen Bestandteilen solcher Regelungen angestellt.

Um Unternehmen bei der Ausarbeitung eigener BCR Hilfestellung zu leisten, hat die Gruppe den nachstehenden Rahmen ausgearbeitet, der zeigen soll, wie eine verbindliche unternehmensinterne Datenschutzregelung mit allen notwendigen Bestandteilen, die in den Arbeitsdokumenten WP 74[3] und WP 108[4] vorgestellt wurden, aussehen könnte.

[1] Arbeitsdokument WP 74: „Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer“, angenommen am 3. Juni 2003. **http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_de.htm**

[2] Arbeitsdokument WP 108: „Einführung eines Prüfungskatalogs für einen Antrag auf Genehmigung verbindlicher unternehmensinterner Vorschriften“, angenommen am 14. April 2005. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_de.htm.

[3] Vgl. Fußnote 1.

[4] Vgl. Fußnote 2.

Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (Binding Corporate Rules - BCR)

HINWEIS

Es handelt sich hier nicht um ein Muster, sondern um einen Vorschlag, wie eine verbindliche unternehmensinterne Datenschutzregelung strukturiert werden und wie sie inhaltlich aussehen könnte.

Die BCR sollten auf die Struktur, Datenverarbeitung, Datenschutzpolitik und -verfahren der jeweiligen Unternehmensgruppe zugeschnitten sein. Die Datenschutzbehörden werden daher eine wortgetreue Wiedergabe des vorliegenden BCR-Rahmens nicht akzeptieren.

Die BCR sind Ausdruck der Datenschutzpolitik, die eine Unternehmensgruppe in Bezug auf die Übermittlung personenbezogener Daten aus der EU verfolgt. Sie können später zur Grundlage für die gesamte Verarbeitung aller Personaldaten in der Unternehmensgruppe werden.

Einleitung:

- Ausdrückliche Verpflichtung aller Mitglieder der Unternehmensgruppe und aller Beschäftigten zur Einhaltung der BCR
- Selbstverpflichtung der Unternehmensleitung, für die Einhaltung der BCR zu sorgen
- Ziele der BCR (angemessener Schutz der personenbezogenen Daten, die von der Unternehmensgruppe übermittelt und verarbeitet werden)
- Verweis auf die geltenden Datenschutzbestimmungen (EU-Richtlinien 95/46/EG und 2002/58/EG)

1 – Anwendungs- und Geltungsbereich

Beschreibung des Anwendungs- und Geltungsbereichs der BCR, u. a.:

- Anwendung auf Übermittlungs- und Verarbeitungsvorgänge innerhalb der Unternehmensgruppe
- Geltungsbereich (nur Verarbeitungsvorgänge innerhalb der EU und Datenübermittlungen aus der EU in Drittländer oder sämtliche Verarbeitungs- und Übermittlungsvorgänge)
- Materieller Anwendungsbereich (z. R. Art der Datenverarbeitung: automatisiert/manuell, Art der Daten: Kunden/Mitarbeiter/Lieferanten)

Allgemeine Beschreibung des Datenverkehrs und der Verarbeitungszwecke einschließlich:

- Art der übermittelten Daten
- Übermittlungs-/Verarbeitungszwecke
- Datenimporteure/-exporteure innerhalb und außerhalb der EU[5]

[5] Manche Datenschutzbehörden verlangen unter Umständen eine ausführlichere Beschreibung der Übermittlungs- und Verarbeitungsvorgänge.

2 – Begriffsbestimmungen

Erläuterung der wichtigsten Begriffe:

- Personenbezogene Daten, sensible personenbezogene Daten, betroffene Person, für die Verarbeitung Verantwortlicher, Datenverarbeiter, Datenverarbeitung, Dritter, Datenschutzbehörden
- Erstellung eines Glossars mit anderen relevanten Begriffen wie Datenexporteur, Datenimporteur, EU-Hauptniederlassung/in der EU haftendes Unternehmen, Mitglied der Unternehmensgruppe[6], Datenschutzbeauftragter/für den Datenschutz zuständige Stelle
- Selbstverpflichtung zur Auslegung der BCR im Sinne der EU-Richtlinien 95/46/EG und 2002/58/EG

3 - Zweckbindung

Beschreibung der Datenverarbeitungs- und übermittlungszwecke und Bestätigung folgender Grundsätze:

- Der Zweck der Verarbeitung und Übermittlung personenbezogener Daten muss eindeutig und rechtmäßig sein.
- Personenbezogene Daten dürfen nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden.
- Für sensible Daten werden zusätzliche Schutzvorkehrungen nach Maßgabe der EU-Richtlinie 95/46/EG getroffen.

4 - Datenqualität und -verhältnismäßigkeit

In den BCR ist folgende Selbstverpflichtung aufzunehmen:

- Personenbezogene Daten müssen sachlich richtig sein und erforderlichenfalls auf den neuesten Stand gebracht werden.
- Personenbezogene Daten sollten den Zwecken entsprechen, für die sie übermittelt oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen.
- Personenbezogene Daten sollten nicht über einen längeren Zeitraum verarbeitet werden, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

5 – Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten sollte auf folgender Grundlage erfolgen:

- Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben oder
- die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen; oder
- die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt; oder

[6] Ein Mitglied kann die Funktion eines für die Verarbeitung Verantwortlichen, eines Datenverarbeiters, eines Datenexporteurs oder –importeurs ausüben.

- die Verarbeitung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich; oder
- die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde; oder
- die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, 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 überwiegen.

6 – Rechtsgrundlage für die Verarbeitung sensibler Daten

Sensible Daten dürfen nur unter folgenden Bedingungen verarbeitet werden:

- 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 Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund des einzelstaatlichen Rechts, 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 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.

7 – Transparenz und Recht auf Information

Selbstverpflichtung, allen betroffenen Personen leichten Zugang zu den BCR zu gewähren

In den BCR sollte darüber hinaus beschrieben sein, wie die betroffenen Personen über die Übermittlung und Verarbeitung ihrer Personaldaten informiert werden.

Selbstverpflichtung zur Unterrichtung der betroffenen Personen vor Verarbeitung ihrer Daten über:

- die Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters
- die Zwecke der Verarbeitung, für die die Daten bestimmt sind,
- sowie über weitere Aspekte wie:
  i) die Datenempfänger oder Kategorien der Datenempfänger
  ii) das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten,

  sofern die Mitteilung dieser weiteren Aspekte unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig ist, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

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.

8 – Recht auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten

In den BCR ist folgende Selbstverpflichtung aufzunehmen:

- Jede betroffene Person hat das Recht, frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten eine Kopie aller sie betreffenden Daten, die Gegenstand einer Verarbeitung sind, zu erhalten.
- Jede betroffene Person hat ein Recht auf Berichtigung, Löschung oder Sperrung von Daten, insbesondere wenn diese Daten unvollständig oder unrichtig sind.
- Jede betroffene Person hat das Recht, jederzeit aus zwingenden, berechtigten Gründen, die mit ihrer persönlichen Situation zusammenhängen, Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzulegen, es sei denn, die Verarbeitung dieser Daten ist gesetzlich vorgeschrieben. Ist der Widerspruch begründet, muss die Verarbeitung dieser Daten eingestellt werden.
- Jede betroffene Person hat das Recht, auf Antrag kostenfrei gegen eine Verarbeitung sie betreffender Daten für Zwecke der Direktwerbung Widerspruch einzulegen.

Erläuterung, wie die betroffenen Personen Auskünfte über ihre personenbezogenen Daten erlangen können

9 – Automatisierte Einzelentscheidungen

Selbstverpflichtung, dass keine Entscheidung, die die betroffene Person erheblich beeinträchtigt, ausschließlich auf eine automatisierte Verarbeitung ihrer Daten gestützt wird, es sei denn,

- 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 Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt.

10 – Sicherheit und Vertraulichkeit

Selbstverpflichtung zur Anwendung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und gegen jede andere Form der unrechtmäßigen Verarbeitung schützen

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Bei der Verarbeitung sensibler Daten sind erhöhte Sicherheitsmaßnahmen vorzusehen.

11 – Verhältnis zu Datenverarbeitern, die der Unternehmensgruppe angehören

Erläuterung, wie personenbezogene Daten geschützt werden, wenn der Verarbeiter der Unternehmensgruppe angehört, insbesondere unter Beachtung folgender Grundsätze:
- 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.
- Der für die Verarbeitung Verantwortliche schließt mit dem Verarbeiter einen schriftlichen Vertrag nach Maßgabe des anwendbaren Rechts, in dem u. a. Folgendes festgelegt ist:
  i) Der Verarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen.
  ii) Die Sicherheits- und Vertraulichkeitsbestimmungen gelten auch für den Verarbeiter.

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

Erläuterung, wie der Datentransfer und die Weiterübermittlung außerhalb der Unternehmensgruppe beschränkt wird, und eine Selbstverpflichtung folgenden Inhalts:
- Mit externen Datenverarbeitern innerhalb der EU oder in einem Land mit einem von der EU-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 sind die EU-Vorschriften für den grenzüberschreitenden Datenverkehr zu beachten (Artikel 25 und 26 der 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).

13 – Schulungsprogramm

Selbstverpflichtung zur Bereitstellung geeigneter BCR-Schulungsmaßnahmen für Mitarbeiter, die ständigen oder regelmäßigen Zugang zu Personaldaten haben, die solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln

14 – Auditprogramm

Selbstverpflichtung, die Einhaltung der BCR innerhalb der Unternehmensgruppe einem Audit zu unterziehen, das u. a. durch folgende Merkmale gekennzeichnet ist:

- Das Auditprogramm erstreckt sich auf alle Aspekte der BCR und sieht Verfahren vor, mit denen sichergestellt wird, dass Abhilfemaßnahmen getroffen werden.
- Datenschutzaudits müssen regelmäßig (zeitliche Vorgabe) durch interne oder durch 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 können eine Kopie dieser Audits anfordern.
- Im Auditplan ist vorzusehen, dass die Datenschutzbehörden bei Bedarf ein eigenes Datenschutzaudit durchführen können.
- Jedes Mitglied der Unternehmensgruppe muss solche Prüfungen der Datenschutzbehörden dulden und deren Mitteilungen, die die Anwendung der BCR betreffen, nachkommen.

15 – Einhaltung der BCR und Überwachung

Selbstverpflichtung des Unternehmens, einen Mitarbeiterstab zu bilden (z. B. ein Netz von Datenschutzbeauftragten), der mit Unterstützung der Unternehmensspitze die Einhaltung der Vorschriften überwacht und gewährleistet

Kurze Beschreibung der Struktur, Aufgaben und Zuständigkeiten des Stabs der Mitarbeiter/Datenschutzbeauftragten o. ä., die die Einhaltung der BCR gewährleisten sollen. Z. B.: Der oberste Datenschutzbeauftragte berät die Unternehmensleitung, ist zuständig bei Untersuchungen der Datenschutzbehörden, 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.

16 – Vorgehen bei einzelstaatlichen Vorschriften, die der Einhaltung der BCR entgegenstehen

Eindeutige Informationspflicht: Hat ein Unternehmen der Gruppe Anlass zu der Annahme, dass die es betreffenden Rechtsvorschriften es daran hindern, seinen Verpflichtungen im Rahmen der BCR nachzukommen, und dass diese Rechtsvorschriften die durch die BCR gebotenen Garantien wesentlich beeinträchtigen, muss es unverzüglich 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 informieren (sofern dem nicht ein Verbot einer Vollstreckungsbehörde entgegensteht, z. B. zur Wahrung des Untersuchungsgeheimnisses in einer Strafsache).

Im Falle einer Kollision zwischen nationalem Recht und den BCR beschließt die EU-Hauptniederlassung, das Unternehmen, das in der EU die Haftung für den Datenschutz übernommen hat, oder der zuständige Datenschutzbeauftragte nach Abwägung aller Argumente über das weitere Vorgehen und zieht im Zweifelsfall die zuständigen Datenschutzbehörden zu Rate.

17 – Interne Beschwerdeverfahren

Selbstverpflichtung zur Einführung eines Beschwerdeverfahrens, das folgenden Grundsätzen genügt:

- Jede betroffene Person muss Beschwerde mit der Begründung erheben können, dass ein Mitglied der Unternehmensgruppe gegen die BCR verstößt.
- Mit den Beschwerden muss sich eine klar bezeichnete Beschwerdeabteilung oder Person befassen, die bei der Wahrnehmung dieser Aufgabe über ein entsprechendes Maß an Unabhängigkeit verfügt.

18 - Drittbegünstigung

Eine klare Aussage dahin gehend, dass die BCR den betroffenen Personen als Drittbegünstigte Durchsetzungsrechte einräumen. Hierzu zählen gerichtliche Rechtsbehelfe

bei Verstoß gegen garantierte Rechte und Schadenersatzansprüche (vgl. Artikel 22 und 23 der EU-Richtlinie).

Erklärung dahin gehend, dass die betroffenen Personen ihre Beschwerde nach Wahl einlegen können:

- am Gerichtsstand des in der EU ansässigen Datenexporteurs,
- am Gerichtsstand der EU-Hauptniederlassung/des haftenden Unternehmens in der EU oder
- bei den zuständigen Datenschutzbehörden.

Selbstverpflichtung, dass die Klausel über die Drittbegünstigung für alle betroffenen Personen, die Rechte als Drittbegünstigte in Anspruch nehmen können, leicht zugänglich ist

19 - Haftung

Aufzunehmen ist eine Selbstverpflichtung folgenden Inhalts:

- Die EU-Hauptniederlassung oder das haftende Unternehmen in der EU[7] übernimmt die Haftung für Handlungen anderer Gruppenmitglieder außerhalb der EU, ergreift die notwendigen Maßnahmen, um Verstößen gegen die BCR abzuhelfen, und leistet Ersatz für Schäden, die aus einem Verstoß gegen die BCR 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 gegen die BCR, 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 zuzurechnen ist.

20 – Gegenseitige Unterstützung und Zusammenarbeit mit den Datenschutzbehörden

Selbstverpflichtung dahin gehend, dass

- die Mitglieder der Unternehmensgruppe bei Anfragen oder Beschwerden einer betroffenen Person oder bei Untersuchungen oder Nachforschungen der Datenschutzbehörden zusammenarbeiten und einander unterstützen die Unternehmen den Mitteilungen der Datenschutzbehörden, die die Auslegung der BCR betreffen, nachkommen.

[7] Ist es im Falle von Unternehmensgruppen mit einer besonderen Struktur nicht möglich, einem Mitglied der Gruppe die Haftung für außerhalb der EU begangene Verstöße gegen die BCR aufzuerlegen, können die 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. 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. 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.

21 – Aktualisierung der Vorschriften

Selbstverpflichtung zur Meldung signifikanter Änderungen der BCR oder der Mitgliederliste gegenüber allen Mitgliedern der Unternehmensgruppe und den Datenschutzbehörden, um Änderungen der gesetzlichen Regelungen oder der Unternehmensstruktur Rechnung zu tragen:

- Für manche Änderungen ist unter Umständen eine neue Genehmigung der Datenschutzbehörden erforderlich.
- Unter folgenden Voraussetzungen sind Aktualisierungen der BCR oder der Liste der Unternehmen, für die die BCR gelten, möglich, ohne eine neue Genehmigung beantragen zu müssen:

  i) Es wird eine Person benannt, die eine stets aktualisierte Liste der Gruppenmitglieder führt, Änderungen der BCR erfasst und den betroffenen Personen oder Datenschutzbehörden auf Anfrage diesbezügliche Auskünfte erteilt.
  ii) Einem neuen Mitglied der Unternehmensgruppe dürfen personenbezogene Daten erst dann übermittelt werden, wenn die BCR für dieses neue Mitglied gelten und die Einhaltung der Vorschriften gewährleistet ist.
  iii) Signifikante Änderungen der BCR oder der Mitgliederliste sollten den für die Genehmigung zuständigen Datenschutzbehörden jährlich mit einer kurzen Begründung der Änderungen gemeldet werden.

Selbstverpflichtung dahin gehend, dass signifikante Änderungen der Vorschriften auch den betroffenen Personen mitgeteilt werden

22 – **Verhältnis zwischen einzelstaatlichem Recht und BCR**

Erklärung, dass
- in Fällen, in denen das geltende Recht – z. B. EU-Recht – ein höheres Schutzniveau für personenbezogene Daten vorschreibt, dieses Recht den BCR vorgeht
- die Datenverarbeitung in jedem Fall nach Maßgabe des anwendbaren Rechts im Sinne von Artikel 4 der Richtlinie 95/46/EG und der einschlägigen einzelstaatlichen Vorschriften erfolgt

23 – Schlussbestimmungen

- Zeitpunkt des Inkrafttretens
- Übergangszeit

Bei den Datenschutzbehörden einzureichende Unterlagen

1 - Antragsformular WP 133
2 - Unterlagen, die Aufschluss über die Einhaltung der BCR geben können, z. B.:

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

- Leitlinien für die Beschäftigten, die Zugang zu personenbezogenen Daten haben, um ihnen das Verständnis und die Anwendung der BCR zu erleichtern (z. B. Leitlinien für den Umgang mit Beschwerden, die Information der betroffenen Personen, für geeignete Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit der Datenverarbeitung)
- Datenschutzauditplan und –programm unter Angabe der zuständigen Personen (interne/externe akkreditierte Auditoren der Unternehmensgruppe)
- Beschreibung des Schulungsprogramms und/oder Beispiele
- 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 BCR entstanden ist
- Beschreibung des internen Beschwerdeverfahrens
- Liste der Unternehmen, die an die BCR gebunden sind
- Sicherheitspolitik in Bezug auf IT-Systeme, mit denen personenbezogene Daten aus der EU verarbeitet werden
- Zertifizierungsverfahren, mit dem gewährleistet ist, dass alle neuen IT-Anwendungen zur Verarbeitung von EU-Daten mit den BCR vereinbar sind
- Musterverträge für Datenverarbeiter (innerhalb oder außerhalb der Unternehmensgruppe), die EU-Daten verarbeiten
- Stellenbeschreibung des Datenschutzbeauftragten oder anderer Personen, die für den Datenschutz in der Unternehmensgruppe zuständig sind.

Brüssel, den 24.6.2008

Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK