



1271-04-02/08/DE
WP 155 Rev.04

Arbeitsdokument zu „Häufig gestellten Fragen“ über verbindliche unternehmensinterne Datenschutzregelungen (BCR)

Angenommen am 24. Juni 2008
Zuletzt überarbeitet und angenommen am 8. April 2009

Diese Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges europäisches Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG und Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von: Europäische Kommission, GD Justiz, Freiheit und Sicherheit, Direktion C (Ziviljustiz, Grundrechte und Unionsbürgerschaft), B-1049 Brüssel, Belgien, Büro LX-46 06/80.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

Häufig gestellte Fragen zu verbindlichen unternehmensinternen Datenschutzregelungen (Binding Corporate Rules - BCR)

Verbindliche unternehmensinterne Datenschutzregelungen (BCR) stellen nach Auffassung der Artikel-29-Datenschutzgruppe, wie in Arbeitsdokument WP 74¹ erläutert, eine geeignete Lösung für multinationale Konzerne und ähnliche Unternehmensgruppen dar, um ihren rechtlichen Verpflichtungen nachzukommen und bei der Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union ein angemessenes Datenschutzniveau zu gewährleisten.

Die Gruppe/Datenschutzbehörden haben anhand ihrer Erfahrungen mit den Anträgen auf Genehmigung unternehmensinterner Datenschutzregelungen und den Anfragen zur Auslegung der Arbeitsdokumente WP 74² und WP 108³ die nachstehende Liste häufig gestellter Fragen zusammengestellt. Anhand dieser Fragen sollen sich die Antragsteller ein klareres Bild von den Anforderungen machen können, so dass sie die Genehmigungsvoraussetzungen für ihre BCR leichter erfüllen können.

Die Liste der häufig gestellten Fragen wird bei Bedarf aktualisiert.

1 – Müssen die verbindlichen unternehmensinternen Datenschutzregelungen auf alle im Unternehmen verarbeiteten personenbezogenen Daten angewandt werden?

Nein, unternehmensinterne Datenschutzregelungen sind rechtlich zulässige Vorkehrungen, um personenbezogene Daten im Sinne der Richtlinie 95/46/EG angemessen zu schützen, wenn sie von der Europäischen Union aus in Drittländer übermittelt werden, deren Datenschutz als unzureichend angesehen wird. Auf andere von dem Unternehmen verarbeitete personenbezogene Daten, die nicht an einem Ort in der EU verarbeitet werden, müssen die unternehmensinternen Vorschriften nicht angewandt werden.

Den multinationalen Unternehmensgruppen, die BCR anwenden, wird jedoch nachdrücklich eine einheitliche Strategie oder Regelung für den Schutz aller im Unternehmen verarbeiteten Personaldaten empfohlen. Eine einheitliche Regelung ist unkomplizierter und effizienter, da ihre Anwendung für das Personal einfacher ist und von den Betroffenen leichter durchschaut werden kann. Auch das Ansehen eines Unternehmens, das sich unabhängig vom Standort und von den jeweiligen rechtlichen Anforderungen entschlossen für den Schutz der Privatsphäre aller betroffenen Personen einsetzt, würde hierdurch gewinnen.

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 Vgl. Fußnote 1.

³ 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.

Es sei darauf hingewiesen, dass es in einem Unternehmen durchaus eine einheitliche Regelung geben kann, die in den BCR geforderten Rechte von Drittbegünstigten jedoch gleichzeitig auf personenbezogene Daten beschränkt sind, die von der Europäischen Union aus in Drittländer übermittelt werden.

2 – Müssen die verbindlichen unternehmensinternen Datenschutzregelungen auf Datenverarbeiter angewandt werden, die nicht der Unternehmensgruppe angehören?

Nein, nur Datenverarbeiter, die der Unternehmensgruppe angehören und Daten im Auftrag anderer Mitglieder der Gruppe verarbeiten, müssen als Mitglied der Unternehmensgruppe die BCR einhalten. Die BCR sollten spezielle Vorschriften für Mitglieder der Unternehmensgruppe enthalten, die als Auftragsverarbeiter tätig sind, um den Anforderungen der Artikel 16 und 17 der Richtlinie 95/46/EG zu genügen.

Datenverarbeiter, die nicht der Unternehmensgruppe angehören und im Auftrag eines Mitglieds der Gruppe tätig sind, müssen nicht den BCR unterworfen werden. Sie sollten allerdings stets nur nach Weisung des für die Verarbeitung Verantwortlichen handeln und gemäß Artikel 16 und 17 der EU-Richtlinie durch Vertrag oder Rechtsakt gebunden sein.

Gehören die Datenverarbeiter nicht der Unternehmensgruppe an und sind sie außerhalb der EU ansässig, müssen die Mitglieder der Unternehmensgruppe außerdem den Artikeln 25 und 26 der Richtlinie 95/46/EG zum grenzüberschreitenden Datenverkehr entsprechen und ein angemessenes Schutzniveau gewährleisten. Das Unternehmen kann beispielsweise die Angemessenheit des Schutzniveaus vertraglich durch Anwendung der Standardvertragsklauseln absichern, die die EU-Kommission für die Datenübermittlung an einen Auftragsverarbeiter außerhalb der EU festgelegt hat, oder die Auftragsverarbeiter den verbindlichen unternehmensinternen Datenschutzregelungen unterwerfen.

Die BCR müssen für solche Situationen eine geeignete Regelung vorsehen.

3 – Wer ist in der Unternehmensgruppe verantwortlich, wenn die BCR außerhalb der EU verletzt werden?

Unabhängig von der in der Richtlinie 95/46/EG vorgesehenen Haftung des Unternehmens, das Personaldaten aus der EU in ein Drittland übermittelt, muss in den BCR selbst ein in der EU ansässiges Mitglied der Unternehmensgruppe benannt werden, das im Fall eines Verstoßes gegen die BCR durch ein Gruppenmitglied außerhalb der EU die Haftung übernimmt. Diese Haftung braucht nicht über den nach Maßgabe der BCR vorgenommenen Datentransfer in Drittländer hinauszugehen.

Im Arbeitsdokument WP 74 wird die Auffassung vertreten, dass die Haftung in der Regel von der Hauptniederlassung der Unternehmensgruppe, sofern sie sich in der EU befindet, übernommen werden sollte. Andernfalls sollte ein in der EU ansässiges Mitglied der Unternehmensgruppe benannt werden, das die Haftung für Verstöße außerhalb der EU übernimmt. Die Haftung würde auch die Leistung von Schadenersatz im Falle eines Verstoßes gegen die verbindlichen unternehmensinternen Datenschutzregelungen durch ein an diese Regelungen gebundenes Mitglied der Unternehmensgruppe außerhalb der EU einschließen.

Für manche Unternehmensgruppen ist es jedoch aufgrund ihrer besonderen Struktur nicht immer möglich, einem bestimmten Unternehmen die Haftung für sämtliche Verstöße gegen die BCR, die außerhalb der EU erfolgen, aufzuerlegen. In diesen Fällen ist die Datenschutzgruppe damit einverstanden, dass eine Unternehmensgruppe eine andere Haftungsregelung, die ihrer Organisation besser entspricht, vorschlagen kann, wenn sie nachweisen kann, dass es ihr nicht möglich ist, ein Mitglied der Unternehmensgruppe in der EU zu benennen.

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.

Solche alternativen Haftungslösungen können von den Datenschutzbehörden im Einzelfall akzeptiert werden, wenn der Antragsteller hinreichende, angemessene Garantien bietet. In diesem Fall ist der Nachweis wichtig, dass die betroffenen Personen bei der Wahrnehmung ihrer Rechte unterstützt und nicht benachteiligt oder in anderer Weise behindert werden.

4 – Müssen die BCR der betroffenen Person stets das Recht gewähren, wegen Verletzung der BCR Beschwerde bei der Datenschutzbehörde zu erheben?

Ja, auch wenn die Regelung oder insbesondere die Drittbegünstigung auf Daten aus der EU beschränkt worden ist und Personen bereits aufgrund ihres innerstaatlichen Rechts berechtigt sind, bei der Datenschutzbehörde Beschwerde gegen den Datenexporteur zu erheben, ist es wichtig, dass in den BCR ein Beschwerderecht verankert ist, wenn ein Mitglied der Unternehmensgruppe gegen die BCR insgesamt verstoßen hat.

5 – Sollen betroffene Personen über ihre Rechte als Drittbegünstigte informiert werden?

Ja, sowohl die unternehmensinternen Datenschutzregelungen als auch die Beschwerdemöglichkeiten und Rechtsbehelfe bei Verstoß gegen die BCR sollten laut WP 74 für die betroffenen Personen leicht zugänglich sein. Die Drittbegünstigung stellt eine wichtige Option für eine betroffene Person dar, die die ihr zur Verfügung stehenden Abhilfen und Rechtsbehelfe prüft. Einige Unternehmen haben aus durchaus berechtigten Gründen beschlossen, die Drittbegünstigungsklausel nicht in den Hauptteil der BCR aufzunehmen, sondern gesondert in einem Dokument aufzuführen. Sind diese Rechte in einem gesonderten Dokument niedergelegt, muss dieses Dokument allen Betroffenen, die sich auf die Drittbegünstigung berufen können, zur Kenntnis gebracht und ohne Umstände zugänglich gemacht werden.

6 – Muss in den BCR selbst auf die Verarbeitung und Übermittlung von personenbezogenen Daten eingegangen werden, und wie detailliert müssen diese Angaben sein?

Ja, die BCR müssen eine allgemeine Beschreibung der wichtigsten Verarbeitungszwecke und Arten der Datenübermittlung enthalten.

Beispielsweise kann in den BCR angegeben werden, dass im Zusammenhang mit der Mobilität des Personals Daten an alle Unternehmen der Gruppe übermittelt werden, dass Personaldaten an die Hauptdatenzentren in Deutschland, den USA und Singapur zur Speicherung und Archivierung übermittelt werden oder dass diese Daten der Konzernspitze mitgeteilt werden, um eine allgemeine Strategie für Löhne und Gehälter und für sonstige Leistungen innerhalb der Unternehmensgruppe festlegen zu können.

Einige Mitgliedstaaten können von den Antragstellern allerdings auch verlangen, dass diese, wenn sie in dem betreffenden Mitgliedstaat einen Antrag auf Genehmigung ihrer BCR stellen, die Übermittlungsvorgänge von diesem Staat aus in Drittländer detailliert beschreiben.

7 – Sollten die BCR in einem Dokument zusammengefasst werden, in dem alle Pflichten der Unternehmensgruppe und die Rechte des Einzelnen geregelt sind?

Den Datenschutzbehörden würde die Überprüfung der BCR erheblich erleichtert, wenn es eine einzige Regelung gäbe, aus der alle Rechte und Pflichten klar hervorgehen. Bei Bedarf könnte diese Regelung ergänzt werden durch andere einschlägige Texte wie Strategiepapiere, Leitlinien, Audit-/Schulungsprogramme. Auf diese Weise könnten die BCR von den Betroffenen auch besser nachvollzogen werden. Ein Beispiel für eine solche Regelung enthält das WP 154 vom 24. Juni 2008, in dem ein Rahmen für verbindliche unternehmensinterne Datenschutzregelungen vorgestellt wird. Es ist jedoch nicht vorgeschrieben, dass die Datenschutzregelungen in einem einzigen Dokument zusammengefasst werden müssen.

8 – Welche Terminologie sollte in den BCR verwendet werden?

Da die BCR nach innen und nach außen Rechtswirkungen entfalten und ein im Sinne der EU-Richtlinie 95/46/EG angemessenes Datenschutzniveau gewährleisten sollen, sollten die Formulierungen und Begriffsbestimmungen der wichtigsten BCR-Prinzipien (siehe WP 74, WP 108, WP 153 und WP 154) denen der EU-Richtlinie entsprechen.

Auf diese Weise wird eine Fehlinterpretation der BCR vermieden und der Datenschutzbehörde wird die Prüfung der BCR erleichtert, deren Begrifflichkeit leichter zu erfassen ist.

Den Unternehmen steht es allerdings frei, andere – gleichbedeutende – Formulierungen zu verwenden, wenn diese bei der Anwendung der BCR im Rahmen der allgemeinen Unternehmensstrategie oder interner Leitlinien für die Mitarbeiter und Kunden einfacher zu verstehen sind.

9 – Welche Rechte sollten einer betroffenen Person nach der Drittbegünstigungsklausel zustehen?

Eine Person, deren personenbezogene Daten auf der Grundlage der BCR verarbeitet werden, kann sich vor der zuständigen Datenschutzbehörde oder dem zuständigen Gericht nach Maßgabe der in den Arbeitsdokumenten WP 74, WP 108 und WP 153 festgelegten Regeln auf die nachstehenden BCR-Grundsätze berufen, um ihre Rechte geltend zu machen und Schadenersatz zu erlangen, wenn ein Mitglied der Unternehmensgruppe seinen Pflichten nicht nachgekommen ist und diese Grundsätze nicht beachtet.

Folgende Grundsätze können im Wege der Drittbegünstigungsklausel geltend gemacht werden:

- Zweckbindung (WP 153 Ziff. 6.1, WP 154 Ziff. 3)
- Datenqualität und -verhältnismäßigkeit (WP 153 Ziff. 6.1, WP 154 Ziff. 4)
- Rechtsgrundlage für die Datenverarbeitung (WP 154 Ziff. 5 und 6)
- Transparenz und einfacher Zugang zu den BCR (WP 153 Ziff. 6.1, Ziff. 1.7, WP 154 Ziff. 7)
- Recht auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten und Recht auf Widerspruch gegen die Verarbeitung (WP 153 Ziff. 6.1, WP 154 Ziff. 8)
- Rechte bei automatisierten Einzelentscheidungen (WP 154 Ziff. 9)
- Sicherheit und Vertraulichkeit (WP 153 Ziff. 6.1, WP 154 Ziff. 10 und 11)

- Beschränkung des Datentransfers außerhalb der Unternehmensgruppe (WP 153 Ziff. 6.1, WP 154 Ziff. 12)
- Einzelstaatliche Vorschriften, die der Einhaltung der BCR entgegenstehen (WP 153 Ziff. 6.3, WP 154 Ziff. 16)
- Interne Beschwerdeverfahren (WP 153 Ziff. 2.2, WP 154 Ziff. 17)
- Pflicht zur Zusammenarbeit mit der Datenschutzbehörde (WP 153 Ziff. 3.1, WP 154 Ziff. 20)
- Haftung und Rechtsbehelfe (WP 153 Ziff. 1.3, 1.4 , WP 154 Ziff. 18 und 19).

Die Unternehmen sollten sicherstellen, dass all diese Rechte in der Drittbegünstigungsklausel ihrer BCR erfasst sind, indem sie beispielsweise auf die Klauseln/Abschnitte/Ziffern ihrer BCR verweisen, in denen diese Rechte geregelt sind, oder indem sie sie alle in der Drittbegünstigungsklausel auflühren.

Diese Rechte erstrecken sich nicht auf BCR-Bestimmungen, die unternehmensinterne Verfahren im Hinblick auf Schulungs- und Auditprogramme, Datenschutzbeauftragte und die Aktualisierung der BCR betreffen. [WP 153 Ziff. 2.1, 2.3, 2.4 und 5.1, WP 154 Ziff. 13 bis 15 und Ziff. 21]

10 – Wie ist das Verhältnis zwischen den EWR-Datenschutzgesetzen und den BCR?

Die BCR treten nicht an die Stelle der nationalen Datenschutzgesetze im EWR, die die Verarbeitung personenbezogener Daten in den EWR-Mitgliedstaaten regeln. Die BCR sollen zwar angemessene Schutzbestimmungen für die Übermittlung solcher Daten bereitstellen, sind aber nicht als eigenständige Regelung anzusehen, die die Datenschutzgesetze im EWR ersetzt. So gilt eine von einem EWR-Mitgliedstaat gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilte Genehmigung ausschließlich für die Übermittlung von Daten aus einem EWR-Land in ein Drittland und bescheinigt deshalb nicht, dass die Verarbeitung im EWR den nationalen Datenschutzgesetzen im EWR entspricht.

11 – Was bedeutet die Beweislastumkehr in der Praxis?

Können betroffene Personen nachweisen, dass sie einen Schaden erlitten haben, der vermutlich durch einen Verstoß gegen die BCR verursacht wurde, ist es Sache des in der EU ansässigen Mitglieds der Unternehmensgruppe, das die Haftung übernommen hat, nachzuweisen, dass das außerhalb Europas ansässige Mitglied der Unternehmensgruppe nicht für den Verstoß gegen die BCR verantwortlich war, durch den der Schaden entstanden ist, bzw. dass kein Verstoß gegen die BCR vorlag.

Brüssel, den 24.6.2008

*Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK*

Zuletzt überarbeitet und angenommen
am 8.4.2009

*Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK*