HELBING
Kanzlei für IT- und Datenschutzrecht

BINDING CORPORATE RULES (BCR) ALS MITTEL ZUR DATEN-SCHUTZ COMPLIANCE

Leitfaden für die Praxis

Rechtsanwaltskanzlei
Dr. Thomas Helbing

www.thomashelbing.com

Königinstraße 11a
80539 München

T +49 (0) 89 - 28 72 465-28
E helbing@thomashelbing.com

USt.-IdNr. DE815182912

EINLEITUNG

Binding Corporate Rules (BCR) sind ein datenschutzrechtliches Instrument, bei dem sich eine Unternehmensgruppe nach bestimmten Vorgaben verbindliche Datenschutzregeln gibt und ein Datenschutzprogramm auferlegt, das die zuständige Datenschutz-Aufsichtsbehörde genehmigt.

Als rechtliche Folge können innerhalb der Unternehmensgruppe personenbezogene Daten leichter von EU-Gesellschaften in Länder außerhalb der EU - sogenannte Drittländer - übermittelt werden. In praktischer Hinsicht sind Binding Corporate Rules dagegen vor allem ein Instrument, um innerhalb von Unternehmensverbünden einheitliche Datenschutzstandards zu schaffen und ein globales Datenschutzprogramm umzusetzen und dies nach außen hin zu zeigen.

Die vorliegende Broschüre behandelt folgende Fragen:

1. Was sind Binding Corporate Rules?
2. Sind Binding Corporate Rules für mein Unternehmen sinnvoll?
3. Was sind die Vor- und Nachteile von Binding Corporate Rules und welche Alternativen gibt es?
4. Welche Schritte sind zur Umsetzung von Binding Corporate Rules nötig?
5. Was ist noch wichtig und welche Fehlvorstellungen gilt es zu vermeiden?
6. Welche Auswirkungen hat die EU Datenschutz-Grundverordnung
7. Wie können Sie uns bei Binding Corporate Rules helfen?
8. Wo erhalte ich weiterführende Informationen?

München, im Juni 2015

Dr. Thomas Helbing
Rechtsanwalt

1. WAS SIND BINDING CORPORATE RULES?

Binding Corporate Rules bezeichnet ein Datenschutzprogramm, das sich eine Gruppe von Unternehmen auferlegt. Im Kern bestehen Binding Corporate Rules aus einer internen Unternehmens-Richtlinie, die den Umgang mit personenbezogenen Daten in Anlehnung an die Europäische Datenschutzrichtlinie regelt. Die Unternehmensgruppe legt sich die Unternehmens-Richtlinie rechtsverbindlich auf, d.h. alle Mitarbeiter müssen an diese gebunden sein (interne Bindung).

Daneben sind den Menschen, deren Daten verarbeitet werden (z.B. Kunden oder Mitarbeitern), bestimmte unmittelbare Rechte einzuräumen, etwa Auskunftsrechte (externe Bindung). Ergänzend ist ein Verfahren für den Umgang mit Beschwerden von Betroffenen festzuschreiben.

Binding Corporate Rules müssen außerdem ein internes Programm zur Datenschutz-Schulung von Mitarbeitern vorsehen und ein Netzwerk von Verantwortlichen für den Datenschutz im Unternehmen implementieren. Daneben sind regelmäßig Kontrollen und Audits der selbstauferlegten Regeln durchzuführen.

2. SIND BINDING CORPORATE RULES FÜR MEIN UNTERNEHMEN SINNVOLL?

Binding Corporate Rules machen zum einen Sinn, wenn eine Unternehmensgruppe ein weltweites Datenschutz-Programm aufsetzen will und hierfür einen „großen Masterplan“ benötigt oder verfolgen will.

Zum anderen lohnen sich Binding Corporate Rules, wenn eine Unternehmensgruppe umfangreich personenbezogene Daten ihrer EU-Gesellschaften an ihre außereuropäischen Unternehmen übermittelt, eine Vielzahl von Gesellschaften und Datentransfers im Spiel sind und sich dabei regelmäßig Änderungen ergeben.

3. WAS SIND DIE VOR- UND NACHTEILE VON BINDING CORPORATE RULES UND WELCHE ALTERNATIVEN GIBT ES?

Binding Corporate Rules sind mehr als auf Papier geschriebene Datenschutzgrundsätze. Binding Corporate Rules beinhalten ein weltweites Datenschutzprogramm mit umfangreich vorgegebenen Inhalten, welche von Aufsichtsbehörden genehmigt werden müssen und deren Umsetzung eine erhebliche und dauerhafte Anstrengung erfordert.

Vorteile:

- **Eine Mission**: Mit dem Entschluss der Unternehmensgruppe Binding Corporate Rules einzuführen wird ein langfristig angelegter Prozess zum Aufbau eines Datenschutzprogramms angestoßen. Die Unternehmensleitung hat ein „Großes Ziel“ vorgegeben, das die Organisation kontinuierlich verfolgt. Das Projekt Binding Corporate Rules rückt den Datenschutz ins Bewusstsein aller Mitarbeiter.
- **Bewährt**: Da Binding Corporate Rules bestimmten Vorgaben genügen und von Aufsichtsbehörden genehmigt werden müssen, ist sichergestellt, dass ein Datenschutzprogramm nach bewährtem Muster und ohne wesentliche Lücken entsteht.
- **Außenwirkung und Akzeptanz**: Binding Corporate Rules signalisieren nach außen hin umfassende Datenschutz-Bemühungen des Unternehmens. Binding Corporate Rules können so auch in der Außendarstellung gegenüber Kunden, Investoren und Lieferanten genutzt werden. Zudem werden Binding

Corporate Rules von Aufsichtsbehörden sehr positiv gewertet.

Nachteile:

- **Starres Korsett**: Die Vorgaben an Binding Corporate Rules sind vergleichsweise umfassend und strikt. Dies kann sich als unflexibel erweisen für Unternehmen, die ihr Datenschutzprogramm klein und überschaubar beginnen wollen.
- **Langes Genehmigungsverfahren**: Die Unternehmensgruppe tritt zwar nur mit einer Datenschutzbehörde in der EU in Kontakt, diese muss aber eine Abstimmung mit allen anderen betroffenen Datenschutzbehörden durchführen. Das ist zeitaufwändig (mindestens 12 Monate) und konfrontiert das Unternehmen mit Vorstellungen unterschiedlichster Behörden. Die EU Datenschutzbehörden sammeln aber zunehmend Erfahrung bei dem Abstimmungsverfahren.

Alternativen und sich daraus ergebende Vor- und Nacheile:

- **EU Standardverträge**: Statt Binding Corporate Rules können die Unternehmen in der EU auch mit den datenempfangenden Unternehmen außerhalb der EU Verträge gemäß den Standardverträgen der EU Kommission für Datenexporte schließen. Je nach Anzahl der beteiligten Gesellschaften kann dadurch eine Vielzahl von Verträgen nötig werden. Durch die Bündelung in Rahmenverträgen kann der Aufwand aber deutlich reduziert werden und dürfte fast immer geringer sein als bei Binding Corporate Rules. Letztlich sind Binding Corporate Rules der umfassendere und nachhaltigere Ansatz. Für schnelle und schlanke Lösungen taugen dagegen auch die Standardverträge.
- **Hausgemachtes Datenschutzprogramm**. Wer die Vorzüge der Einfachheit von Standardverträgen und des umfassenden Compliance Ansatzes der Binding Corporate Rules kombinieren will, kann einen Datenschutz-Rahmenvertrag mit den EU Standardvertragsklauseln abschließen und dazu eine konzernweite Datenschutzrichtlinie erlassen, bei der die Binding Corporate Rules Vorgaben als Blaupause dienen. So kann schnell und effizient ein Datenschutzprogramm ohne behördliche Genehmigung aufgebaut werden.
- **Safe Harbor**. Für Datentransfers aus der EU in die USA – und nur dorthin – kann sich das US Unternehmen gemäß dem Safe Harbor Programm selbst zertifizieren. Es müssen dann keine EU Standardverträge geschlossen werden. Die teils ungünstigen Klauseln zur Haftung und Aufsicht in den Standardverträgen werden vermieden. Safe Harbor funktioniert aber nur bei US Unternehmen bestimmter Branchen. Außerdem wird die Safe Harbor Lösung von deutschen Aufsichtsbehörden zunehmend kritisch gesehen und die EU Kommission verhandelt mit den USA derzeit deren Rahmen neu.

4. WELCHE SCHRITTE SIND ZUR UMSETZUNG VON BINDING CORPORATE RULES NÖTIG?

Schritt 1 - Die Entscheidung: Die Unternehmensgruppe evaluiert Vor- und Nachteile von Binding Corporate Rules sowie Alternativen und entscheidet sich für deren Einführung. Diese Entscheidung muss vom gesamten Vorstand und Top-Management mitgetragen werden („Tone from the Top“)

Schritt 2 - Kontakt mit der Datenschutzbehörde: Das Unternehmen identifiziert die für sie zuständigen verfahrensführende Aufsichtsbehörde (Lead Authority) und tritt mit dieser in Kontakt, um die Zuständigkeit zu klären (Dauer: ca. 2-4 Wochen).

Schritt 3 - Entwurf der Binding Corporate Rules: Das Unternehmen entwirft ein

Dokument, das die verbindlichen Regelungen zum Umgang mit personenbezogenen Daten festlegt,sowie eine Reihe begleitender Unterlagen (z.B. Trainingskonzept, Organisation von Datenschutzverantwortlichen, Auditierungen). Hierzu ist eine umfassende Analyse der Datenflüsse sowie bereits vorhandener Datenschutzmechanismen im Unternehmen und ein Abgleich mit den Vorgaben für Binding Corporate Rules nötig. (Dauer: Unternehmensabhängig, ca. 2 bis 9 Monate)

Schritt 4 - Einreichung und Erstprüfung: Das Unternehmen reicht die Dokumente bei der verfahrensführenden Aufsichtsbehörde ein, diese prüft die Unterlagen und gibt erste Rückmeldungen, die das Unternehmen in die Entwürfe integriert. Es entsteht ein konsolidierter Entwurf.

Schritt 5 - Kommentierung: Die Aufsichtsbehörde zirkuliert den konsolidierten Erstentwurf an die Datenschutzbehörden der anderen EU-Länder, von denen aus die Gruppe Daten in Drittländer exportiert. Diese Aufsichtsbehörden geben ihre Kommentare an die verfahrensführende Aufsichtsbehörde (Dauer ca. einen Monat). Diese konsolidiert die Rückmeldungen und gibt sie an das Unternehmen zurück. Soweit nötig werden von diesem noch in Absprache mit der verfahrensführenden Aufsichtsbehörde Anpassungen vorgenommen. Das Ergebnis ist der finalisierte Entwurf.

Schritt 6 - Genehmigung. Die verfahrensführende Aufsichtsbehörde zirkuliert den finalisierten Entwurf an die anderen Datenschutzbehörden, die ihre Freigabe erteilen. An diesem Verfahren der gegenseitigen Anerkennung (Mutual Recognition) nehmen derzeit 21 EU Länder Teil.

Schritt 7 – Umsetzung. Die einzelnen Unternehmen der Gruppe passen ihre Organisation, Datenverarbeitung und Prozesse gemäß den neuen Unternehmensrichtlinien an („BCR Readiness“) und erklären

5. WAS IST NOCH WICHTIG UND WELCHE FEHLVORSTELLUNGEN GILT ES ZU VERMEIDEN?

Nur interne Datentransfers: Binding Corporate Rules erleichtern nur Datentransfers zwischen Unternehmen einer Unternehmensgruppe. Bei Datenübermittlungen an Externe, zum Beispiel einen externen IT-Provider, helfen sie nicht.

Beschränkung möglich: Die Unternehmensgruppe kann die Anwendung von Binding Corporate Rules zunächst auf bestimmte Datenarten (z.B. nur Kundendaten, keine Mitarbeiterdaten) beschränken, Binding Corporate Rules können aber auch auf solche Daten beschränkt werden, die aus der EU in Drittstaaten exportiert werden, so dass rein „lokale“ Verarbeitungen in der EU oder in Drittstaaten nicht den selbstauferlegten Regeln unterliegen.

Genehmigungen weiter nötig: In einigen Ländern sind für Datenexporte in Drittländer trotz Binding Corporate Rules noch zusätzliche Genehmigungen der lokalen Datenschutzbehörden nötig.

Kein „freier Datenfluss“: Binding Corporate Rules gestatten keinen „freien Datenfluss“ innerhalb des Konzerns. Es muss weiterhin für jede Datenübermittlung eine gesetzliche Erlaubnisnorm vorliegen. Binding Corporate Rules bewirken rechtlich nur, dass die nicht EU Gesellschaften wie solche in der EU behandelt werden.

Auftragsdatenverarbeitungsverträge weiterhin nötig: Binding Corporate Rules befreien nicht davon, Auftragsdatenverarbeitungsverträge innerhalb der Unternehmensgruppe zu schließen, wenn zum Beispiel eine Konzerngesellschaft für die anderen Konzernunternehmen IT-Services erbringt.

Konzerninterne Verträge nötig: Konzerninterne Verträge lassen sich bei Binding Corporate Rules auch deshalb nicht vermeiden, weil Verträge mit der Muttergesellschaft geschlossen werden müssen, um Betroffenen unmittelbare Rechte einzuräumen (externe Bindung, Verträge zu Gunsten Dritter).

Weniger Papier, mehr Aufwand: Im Vergleich zum Abschluss von EU Standardverträgen sorgen Binding Corporate Rules für „weniger Papier“ aber nicht für weniger Aufwand.

Aufwand der Umsetzung wird unterschätzt: Mit der Genehmigung der Binding Corporate Rules beginnt die Arbeit erst: Die Umsetzung der Vorgaben, zum Beispiel in Bezug auf Schulungen und den Aufbau einer entsprechenden Datenschutz-Organisation verursachen einen oft unterschätzen Aufwand. Das Andocken an eine bestehende Compliance Organisation kann hierbei helfen.

Verweigerer und Nachzügler: Im Unternehmensverbund gibt es oft Gesellschaften, bei denen es mit der Umsetzung hapert. Für diese bedarf es dann einer ggf. übergangsweisen alternativen Lösung, zum Beispiel über EU Standardvertragsklauseln.

6. WELCHE AUSWIRKUNGEN HAT DIE EU DATENSCHUTZ-GRUNDVERORDNUNG

Auf EU Ebene ist eine Reform des Datenschutzrechts durch Erlass einer EU-Datenschutz-Grundverordnung geplant. Europa hätte dann statt nationaler Gesetze einen einheitlichen Gesetzestext für den Datenschutz.

Aktuell (Anfang Juni 2015) liegt ein Entwurf für eine Datenschutz-Grundverordnung der EU-Kommission vom 25. Januar 2012 und ein Entwurf des EU-Parlaments vom 12. März 2014 vor. Zudem steht der Rat, in welchem die Vertreter der Regierungen der Mitgliedsstaaten sitzen, kurz vor der Einigung über seinen Vorschlag. Ab Mitte Juni soll der Einigungsprozess zwischen Rat, Parlament und Kommission beginnen, der sogenannte Trilog. Nach aktuellen Planungen könnte dieser bis Ende 2015 abgeschlossen sein. Da der Entwurf eine zweijährige Übergangsfrist vorsieht, würde das neue Recht frühestens ab Anfang 2018 gelten.

Nach den Fassungen der Kommission und des Parlamentes werden die Grundlagen für Binding Corporate Rules in der Verordnung gesetzlich verankert und das Instrument damit insgesamt gestärkt. Das Erfordernis zusätzlicher Genehmigungen für Datentransfers auf Basis von Binding Corporate Rules soll zum Beispiel entfallen, der Prozess der Abstimmung unter den Aufsichtsbehörden gestrafft werden. Zudem ist ein konkreter gesetzlicher Anforderungskatalog an Binding Corporate Rules vorgesehen.

Wer derzeit die Einführung von Binding Corporate Rules plant, sollt sich von den Reformbemühungen auf EU Ebene nicht abhalten lassen: Bis die Regeln greifen, vergeht aufgrund der Übergangsregelung zum einen noch einige Zeit und nach Inkrafttreten dürfen Aufsichtsbehörden ohnehin alle Hände voll zu tun haben. Zum anderen können Organisationen mit bereits eingeführten Binding Corporate Rules die neuen EU Regeln für den Datenschutz (z.B. etwaige Datenschutzfolgeabschätzungen), leichter umsetzen, da sie bereits über entsprechende Strukturen verfügen (Datenschutzbeauftragte, Richtlinien, Schulungen und Audits).

Bei einer jetzigen Konzeption von Binding Corporate Rules sollte aber der Gesetzgebungsprozess auf EU Ebene genau beobachtet werden. Eine Anpassung der internen Richtlinien zum Datenschutz und damit eine Änderung bestehender Binding Corporate Rules dürften unumgänglich werden sobald das neue Regelwerk greift. Wer sich noch etwas Zeit nimmt und den finalen Text der EU Datenschutz-Grundverordnung abwartet, könnte versuchen, die neuen EU Regeln bereits in seinen Binding Corporate Rules vorausgreifend zu integrieren.

8. WO ERHALTE ICH WEITERFÜHRENDE INFORMATIONEN?

Ich kann Sie auf allen Stufen der Umsetzung von Binding Corporate Rules beraten und unterstützen, zum Beispiel bei der Entscheidung Für und Wider Binding Corporate Rules, der Vorbereitung der einzureichenden Unterlagen, der Kommunikation mit der Behörde und bei der späteren Umsetzung der selbstauferlegten Richtlinien im Unternehmen.

Daneben kann ich für Sie alternative Lösungsansätze, z.B. mittels Rahmenverträge konzipieren und umsetzen.

8. WO ERHALTE ICH WEITERFÜHRENDE INFORMATIONEN?

Zu den Binding Corporate Rules haben die Datenschutzbehörden der EU im Rahmen der Artikel 29 Arbeitsgruppe eine Vielzahl von Informationen veröffentlicht. Zum Vertiefen empfehle ich folgende Lektüre und zwar in dieser Reihenfolge:

Für das Erstellen der einzureihenden Unterlagen selbst sind wichtig:

- **Tabelle der Binding Corporate Rules Anforderungen** (WP 153), umfasst eine Liste der Elemente, die alle Binding Corporate Rules enthalten müssen. Es handelt sich um Zusammenfassungen der Dokumente WP 74 und WP 108.
- **Rahmen Binding Corporate Rules** (WP 154) mit einem Vorschlag, wie Binding Corporate Rules aussehen können. Der Vorschlag enthält alle notwendigen Elemente aus den Dokumenten WP 74 und WP 108.
- **Fragen-Antworten-Liste** (WP 155 rev04) mit den wichtigsten Fragen und Antworten zu Binding Corporate Rules, etwa zur Frage der Haftungsregelung.

Für das Verfahren der Freigabe durch Aufsichtsbehörden und die Einreichung der Dokumente relevant:

- **Standard Formular zur Einreichung** von Binding Corporate Rules (WP 133 / Wordfile Englisch)
- **Mutual Recognition**: Beschreibung des Verfahrens der gegenseitigen Anerkennung zwischen den Aufsichtsbehörden (WP 107)

Die grundlegenden Anforderungen sind in den folgenden Dokumenten enthalten. Die Vorgaben sind in den oben genannten (späteren veröffentlichten) Dokumenten bereits berücksichtigt:

- **Ausgangsdokument** „Binding Corporate Rules als Mittel für internationale Datentransfers“ (WP 74) ist quasi die Geburtsurkunde der Binding Corporate Rules
- **Anforderungsliste** für Binding Corporate Rules (WP 108)

Zur Abgrenzung „Processor Binding Corporate Rules“:

Die folgenden Dokumente enthalten Informationen zu „Processor Binding Corporate Rules“, die nicht Gegenstand dieses Beitrages sind. Processor Binding Corporate Rules sind für Unternehmensgruppen gedacht, die im Auftrag anderer Unternehmen *fremde* Daten als *Auftragsdatenverarbeiter* verarbeiten und hierbei *innerhalb ihrer Gruppe* Daten von der EU in Drittländer exportieren (z.B. IT Anbieter in der EU mit ausländischen Töchtern, Rechenzentren oder Headquarter in den USA): WP 195, WP 195a (Wordfile / Englisch).

Rechtsanwaltskanzlei
Dr. Thomas Helbing

Königinstraße 11a
80539 München

T +49 (0) 89 - 28 72 465 - 28
E helbing@thomashelbing.com
www.thomashelbing.com