International Chamber of Commerce
The world business organization

ICC report on binding corporate rules for international transfers of personal data

Prepared by the
ICC Task Force on Privacy and Protection of Personal Data

Christopher Kuner, Chair
Robert Bond, Chair, BCRs Working Group

International Chamber of Commerce
38, Cours Albert 1er, 75008 – Paris, France
Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59
Web site www.iccwbo.org E-mail icc@iccwbo.org

28 October 2004 MvdL/ami
Doc. 373-22/115

TABLE OF CONTENTS

Executive summary

The growing legal restrictions on data transfers between jurisdictions make it necessary to have workable legal bases for such transfers. Although existing legal bases are useful in many cases, they are often too ad hoc for businesses frequently involved in global transfers of data – especially for businesses who regularly transfer data between corporate groups.

Binding corporate rules (BCRs) are a set of rules adopted within a particular company or corporate group that provide legally-binding protections for data processing within the company or group. They offer a more holistic approach to providing a legal basis for global data transfers. However, as there is legal uncertainty about the binding nature of BCRs, many companies have been reluctant to use them to date.

To learn more about the legal enforceability of BCRs around the world, ICC carried out a survey of companies around the world in early 2004 about enforceability in their home jurisdictions. Eighteen responses were received, and respondents included US, UK, Spanish, Swiss, Danish, Belgian, and Hong Kong law firms, and Swiss, Dutch, German, Japanese, and US manufacturing companies and financial services companies.

The responses show that uncertainties remain about the legal enforceability of unilateral declarations in some jurisdictions in the context of BCRs. Governments should work with business to eliminate these uncertainties. Nonetheless, the ICC survey demonstrates that there is a wide variety of legal principles which may lead to legal enforceability of BCRs, and that BCRs are therefore a realistic mechanism for providing a legal basis for data transfers in many jurisdictions around the world.

1 Introduction

ICC strongly supports the fundamental rights to privacy and data protection, as well as compliance by business with national and international privacy laws. Global business believes that appropriate privacy protection is a business enabler, not a barrier. Privacy protection can be a means to develop consumer confidence and trust, and develop lasting and fruitful customer relationships. As the international business organization, with thousands of member companies and organizations in over 130 countries, ICC is working towards a seamless, global legal framework for international transfers of personal data.

In 1995, the European Parliament passed the "Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data". This directive is designed to protect the individual right to privacy with respect to the processing of personal data.[1] It includes restrictions prohibiting the transfers of data to a third (i.e. non-EU) country unless the country in question ensures an adequate level of protection or the company making the transfer complies with a specific derogation. Since the passage of the Directive, countries in other regions, such as Asia[2] and Latin America,[3] have adopted similar restrictions, and still others, such as the US, [4] are considering "adequacy" restrictions close to the European model.

Nine years after the passage of the EU Directive, uncertainty about achieving compliance with legal restrictions on international data transfers can clearly be a barrier to international commerce. Restrictions can be particularly costly for multi-national companies that frequently need to transfer data between different corporate groups. These groups cannot currently use a single data processing standard across all their operations worldwide because they have to comply with a myriad of data transfer regimes.

---

[1] Directive 95/46/EC of the European Parliament and of the Council, Oct. 24, 1995, Art 1 § 1.

[2] For example, Hong Kong enacted the Personal Data (Privacy) Ordinance in 1995. Malaysia and Thailand are in the process of drafting privacy legislation. India has legislation pending that is largely based on the United Kingdom Data Protection Act. In Russia, the Law on Information of Personal Character, which would update the 1995 Act to comply with a number of European Conventions, is currently pending.

[3] Chile was the first country in Latin America to enact privacy legislation when the "Law for the protection of Private Life," was passed in 1999. Argentina enacted its Habeas Data Act, in 2000. A data privacy bill has been pending in Brazil's senate since 1996, although the 1990 Code of Consumer Protection and Defense provides some degree of protection for personal and consumer data stored in files, registries and databases. In both Peru and Mexico, data protection legislation has been introduced but is still pending in Congress.

[4] For example, Bill H.R. 4366 (the "Personal Data Offshoring Protection Act of 2004"), has been introduced in the U.S. federal House of Representatives. Under the Bill, "A business enterprise may transmit personally identifiable information regarding a citizen of the United States to any foreign affiliate or subcontractor located in a country that is a country with adequate privacy protection, provided that the citizen has been provided prior notice that such information may be transmitted to such a foreign affiliate or subcontractor and has not objected to such transmission." Transfers to countries without adequate protections would be prohibited unless the company disclosed the nature of the transfer to the citizen and obtained consent.

What are 'codes of conduct' and 'binding corporate rules'?

Although the terms "code of conduct" and "binding corporate rules" (BCRs) are sometimes used interchangeably, they refer to different devices.

Codes of conduct

A code of conduct may be a single document or an organization-wide set of documents that set out how personal information should be treated, particularly within a certain business sector.

Codes of conduct and BCRs may be developed and made binding in many different ways:

- Under the EU Data Protection Directive,[5] trade associations and other bodies may adopt "codes of conduct" for use in a particular sector. A code of conduct developed by the Federation of European Direct Marketing (FEDMA) has been approved by the European Commission. It clarifies compliance with the Directive on specific direct marketing issues such as the protection of children.[6]

- Codes of conduct can be made binding through membership of an organization or through statutory authority. The British Banker's Association's *Business Banking Code* and the Better Business Bureau *Code of Advertising* are examples of codes whose binding nature derives solely from voluntary membership of the association.

- Codes of conduct can be made enforceable by regulatory authorities, particularly in the financial services industry, e.g. the Swiss Bankers' Code of Conduct is enforceable by regulatory authorities.

- Non membership or statutory based codes of conduct, such as BS7799 and ISO 17799, are generally only binding through their incorporation into contracts.

- One of the few instances of a code that may be binding without membership or statutory authority on a purely voluntary basis is the ICC's standard trade definitions used for international contracts known as INCOTERMS.[7]

For an extensive list of various codes of conduct and their binding nature, see Appendix A.

---

[5] Directive 95/46/EC of the European Parliament and of the Council, Oct. 24, 1995, Art 27 § 1, 2.

[6] "Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing" Article 29 Data Protection Working Party, Adopted on 13 June 2003, 10066/03/En final, "WP77", page 4.

[7] In St. Paul Guardian Insurance Co. et. Al. v. Neruomed Medical Systems & Support, 2002 U.S. Dist. LEXIS 5096 (S.D.N.Y. Mar. 26, 2002), the court held that the dispute over the contract should be interpreted according to the ICC's INCOTERMS even though INCOTERMS were not explicitly referenced by the contract because INCOTERMS are widely known and observed in international trade as standard definitions for delivery terms.

Binding corporate rules (BCRs)

BCRs are a set of rules adopted within a particular company or corporate group that provide legally-binding protections for data processing within the company or group. BCRs can be legally binding on members of a corporate group through a variety of legal devices, and may provide a legal basis for data transfers to other countries or regions.[8]

BCRs are much more than guidelines; they are a tool to facilitate data transfers and improve compliance with data protection laws. Companies have begun adopting BCRs as a legal basis for data transfer, and are having them approved by data protection authorities (DPAs).

The concept of BCRs is not new. Many if not most multinational corporations use BCRs for a variety of compliance requirements such as environmental, health & safety, money laundering and general corporate governance requirements.

Specific examples include the following:

- Investment banks use "Chinese walls," "restricted lists," and "watch lists" to prevent insider trading.
- U.S. defense contractors abide by the *Defense Industry Initiatives on Business Ethics and Conduct* to reduce waste and fraud.
- Large manufacturers employ binding *Environmental Protection Guidelines* to define environmental policy and assess in advance the ecological implications of production processes and products.

In the context of data protection, BCRs are an innovative tool to protect the privacy of data subjects while facilitating international global transfers of personal data to corporate groups in countries without sufficient data protection legislation. BCRs allow companies to transfer personal data around the world using a single set of rules. This gives data subjects the confidence that their personal data is being processed using a binding and enforceable set of standards. BCRs can also simplify the approval of data transfer mechanisms by DPAs. BCRs can facilitate data flows for companies, reduce their uncertainty about compliance, reduce administrative burdens on DPAs and increase the confidence of data subjects.

However, there is significant confusion about the benefits, feasibility, implementation and enforcement of BCRs. This paper aims to dispel such confusion by:

- Explaining the current methods of compliance;
- Highlighting the benefits and limitations of BCRs;
- Explaining how to draft and implement BCRs;
- Analyzing how rules can be made binding in different jurisdictions based on the results of a survey conducted by ICC.

[8] The EU's Article 29 Working Party, which is a group of data protection regulators, suggests such instruments be called "binding corporate rules for international data transfers" or "legally enforceable corporate rules for international data transfers. "Working Document (WP74) adopted by the Article 29 Working Party on June 3, 2003 on "Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers", page 8.

2 Compliance methods for international data transfers

Multi-national companies frequently need to transfer personal data globally to other members of their corporate groups. Compliance with legal rules, such as Articles 25 and 26 of the European Union's Data Protection Directive 95/46, which restrict global data transfers, presents challenges and uncertainties for many companies. The rules of the Directive will be referred to throughout this paper as the leading example of legislative restrictions on the transfer of personal data outside national borders, but the remarks made here are broadly applicable to similar systems in other legal systems as well.

According to the Directive, businesses can transfer data to countries outside of the EU only if the target country has been determined to have adequate privacy protection legislation (Article 25) or if the business complies with a specific derogation (Article 26.) There are several ways to satisfy these restrictions, and many companies have found solutions that fit their own needs. Nonetheless, several outstanding issues can make compliance uncertain, costly and impractical for multi-national corporations, with little clear benefit to data subjects. This difficulty can be better understood by examining some of the most frequently-used legal bases for transferring personal data in the EU Directive, which are also applicable to similar provisions in other legal systems.

Transfers to countries with adequate privacy protection – Article 25

Companies can transfer personal data to countries determined to have adequate privacy protection legislation. To date, only Argentina, Canada, Guernsey, the Isle of Man, Switzerland, and organizations in the US Safe Harbor system have been found adequate.[9] Even if a country is certified as having adequate privacy protections, diverging implementations of Article 25 by member states create uncertainty. For example, EU member states differ on which authorities can make adequacy findings, their treatment of pending adequacy findings, and their recognition of a European Commission adequacy finding.

Unambiguous consent of the data subject – Article 26 § 1(a)

Personal data can be transferred to a third country without adequate data protection if "the data subject has given his consent unambiguously to the proposed transfer."[10] However, European DPAs have restricted the application of the consent requirement by requiring unambiguous, specific, and informed consent.[11] It is practically impossible to obtain unambiguous consent from every data subject prior to every intended transfer.[12]

Adding further confusion, member states treat the issue of consent differently. For example, the concern that the employer/employee relationship prevents employees from

[9] "Commission decisions on the adequacy of the protection of personal data in third countries." The European Commission Internal Market, available at http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm.

[10] Directive 95/46/EC of the European Parliament and of the Council, Oct. 24, 1995, Art 26 § 1(a).

[11] See Working Document (WP12) adopted by the Article 29 Working Party on July 24, 1998, 2003 on "Transfers of Personal Data to Third Countries – Applying Articles 25 and 26 of the EU Data Protection Directive", page 24.

[12] Japan Business Council in Europe, "JBCE Comments on Review of the EU Data Protection Directive 95/46/EC", Jan. 2003, page 4.

truly consenting can prevent consent being used to transfer employee data outside the EU. Since a large percentage of EU personal data transfers contain employee data,[13] restrictions on the use of consent to transfer such data are particularly burdensome.

Necessary for the performance of a contract – Article 26 § 1(b), (c)

Personal data can be transferred to a third country without adequate data protection if "the transfer of data is necessary for the performance of a contract between the data subject and controller"[14], or if "the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party."[15] However, these derogations are often difficult to apply. It is frequently impractical for a company to contract with every data subject prior to a transfer. Also, most member states have strictly limited these derogations to essential data necessary for the precise purpose of the contract.

Contracts giving an adequate level of protection – Article 26 § 2, 4

Personal data can be transferred to a third country without adequate data protection by using standardized contracts[16] drafted by the European Commission or negotiated (ad hoc) contracts[17] that give adequate safeguards with respect to the protection of privacy. However, the Commission's contract clauses are often impractical for businesses because they lack flexibility, while their use can require hundreds (or thousands) of contracts between the various corporate members, which is hardly practical.

In July 2004, ICC and six other leading business organizations proposed a set of "Alternative Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries" for approval by the European Commission. These clauses are designed to provide the same level of data protection as the existing EU clauses, but by using innovative new mechanisms. It is hoped that the alternative standard contractual clauses will be approved by the Commission in the near future.

---

[13] For example, approximately 40% of data transfers out of Italy are employee data. Italian Data Protection Authority ("the Garante") survey published in May 23 Newsletter, available at http://www.garanteprivacy.it/garante/doc.jsp?ID=1006024.

[14] Directive 95/46/EC of the European Parliament and of the Council, Oct. 24, 1995, Art 26 § 1(b).

[15] *Id.*, Art 26 § 1(c).

[16] *Id.*, Art 26 § 4.

[17] *Id.*, Art 26 § 2.

Safe Harbor

Although the EU has not made a finding of adequate protection with regard to the U.S. as a whole, a company in the EU (or an EU subsidiary) can transfer specific categories of data to a U.S. company if that company is a member of the U.S. Department of Commerce's "Safe Harbor" list in respect of those specific categories of data. To be a member of the U.S. Safe Harbor list, which is made public by the U.S. Department of Commerce, a company must certify that it provides adequate privacy protection as defined by the EU Data Protection Directive. The U.S. Federal Trade Commission or a comparable and relevant U.S. government agency (e.g. the Department of Transportation with respect to air carriers and ticket agents) can take enforcement action against organizations that fail to live up to their data protection statements.

Data transfer restrictions in selected non-EU countries

The Habeas Data Act of Argentina appears to be even more stringent than the EU Directive. It does not appear to provide – either explicitly or implicitly – for the use of BCRs to allow global data transfers. Under the Act, the transfer of any type of personal information is prohibited to countries or international or supranational entities that do not provide adequate levels of protection.[18] The only exceptions are transfers necessary for international judicial cooperation,[19] exchange of medical information necessary for the treatment of the affected party,[20] stock exchange and banking transfers,[21] transfers made between intelligence agencies in the fight against organized crime, terrorism, and drug-trafficking,[22] and occasions when the transfer is arranged within the framework of international treaties of which Argentina is a signatory.[23]

Restrictions on international data transfers also exist in Russian law. Article 8 of the Federal Law No. 85-FZ of July 4, 1996 on Participation in the International Information Exchange limits the transfer of documents containing "confidential information" outside the Russian Federation. Confidential information is defined as documented information to which access is restricted in accordance with Russian legislation (such as employee data regulated by the Labour Code). Whether such information may be transferred outside the Russian Federation is to be determined by the Russian government on a case-by-case basis. Further, Law No. 85-FZ specifies limits on the removal of documents from the territory of the Russian Federation by granting access to users located outside of the Russian Federation or by granting access to information systems or networks located within the territory of the Russian Federation.

---

[18] Habeas Data Act, Art. 12 §1 (2000).

[19] *Id.*, Art. 12 §2(a) (2000).

[20] *Id.*, Art. 12 §2(b) (2000).

[21] *Id.*, Art. 12 §2(c) (2000).

[22] *Id.*, Art. 12 §(e) (2000).

[23] *Id.*, Art. 12 § (d) (2000).

Hong Kong's Personal Data (Privacy) Ordinance restricts transfers of personal data outside of Hong Kong unless the destination has laws substantially similar to Hong Kong's,[24] the data subject has consented in writing,[25] or the transfer is for the avoidance or mitigation of adverse action against the data subject and it is not practical to obtain written consent from the data subject.[26] The data controller may make a transfer if he "has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under this Ordinance."[27] This final method of compliance would seem to provide for the possible use of BCRs even though the Ordinance does not explicitly recognize BCRs.

Summary

More and more jurisdictions are enacting restrictions on international data transfers. While such restrictions usually have exemptions for companies to transfer personal data in certain cases, this leads to a piecemeal approach that is inefficient and difficult to administer. Both data controllers and data subjects would benefit from a more uniform, holistic approach to data transfers that allowed them to be conducted under a single legal standard throughout the corporate group. This need has led many companies to explore the use of binding corporate rules.

---

[24] Personal Data (Privacy) Ordinance), 33 §2(a), 3 (1995).

[25] *Id.*, 33 §2(c) (1995).

[26] *Id.*, 33 §2(d) (1995).

[27] *Id.*, 33 §2(f) (1995).

3 Use of binding corporate rules

Benefits of binding corporate rules

BCRs facilitate data transfers between corporate groups

Similar to the "Safe Harbor" that exists for US companies for data transfers from the EU, BCRs can create a "Safe Haven" within an organization for transfers between corporate groups. To create a safe haven, all group companies must be bound by the BCRs that apply the criteria for legitimate processing of personal data. The advantage of BCRs is that a company does not need to apply restrictive criteria for transfers of personal data between corporate groups. Rather, the entire corporate group becomes a "safe haven" in which personal data can be freely transferred from one corporate member to another, receiving the same protection wherever it goes.

BCRs make compliance less time-consuming and costly, and provide multi-national corporations with greater flexibility. Depending on the interpretation of the law by the DPA, the company may or may not need to notify the DPA every time it transfers new data to another corporate group. Also, the company does not need to conclude (and keep track of) thousands of contracts between its corporate members. Instead, it must simply comply with the internal and binding data protection rules uniquely tailored to its business transactions to transfer data between corporate members.

BCRs benefits data subjects by improving compliance with data protection law

BCRs benefit data subjects by increasing compliance with data protection legislation. The 2003 implementation report by the European Commission on Directive 95/46/EC showed "very patchy compliance by data controllers" with the national implementations of the Directive, due in particular to the complex and burdensome nature of data protection law.[28]

The current system is designed to bring compliance through the threat of punitive measures – whether audits by the DPAs or complaints by data subjects. In contrast, BCRs represent a proactive approach to data protection. BCRs shift the burden of ensuring compliance from DPAs and individuals to companies themselves. Use of BCRs also creates and sustains a company culture that respects the privacy of data subjects and promotes compliance with data protection legislation.

[28] "Report from the Commission: First report on the implementation of the Data Protection Directive: Analysis and impact study on the implementation of Directive EC 95/46 in Member States", May 15 2003, page 13.

Limitations of binding corporate rules

Legal limitations of BCRs

Although BCRs create a "safe haven" for transfers between corporate groups, the "safe haven" does not apply to transfers to companies outside of the corporate group ("onward transfers"). BCRs are also both a minimal and complementary standard. So, if local law is stricter than the BCRs, a data subject's claim can be based on local law as the BCRs are only the minimum level of protection. However, if the BCRs offer greater protection than local law, a data subject's claim can be based on them rather than the local law. BCRs therefore have the potential to increase a company's potential liability.

Practical issues with BCRs

The main obstacle to the use of BCRs is the absence of a streamlined mechanism for approval by DPAs. For example, in the EU a company currently has to submit its BCRs for approval to the DPA of each member state from which the company intends to transfer the data (except in the UK where submission is voluntary).[29] Not only is this process time consuming, but the company may also receive demands for twenty-five different versions of its BCRs because each EU Member State has the authority to require changes. Further, some DPAs are very cautious about the use of BCRs in the first place. It may therefore be difficult for a company to get approval of its BCRs by all EU member states.

---

[29] So far, BCRs have been approved by European DPAs in Austria (an unnamed Austrian bank) and Germany (Daimler Chrysler and GE); approval of other companies' BCRs is known to be imminent in other Member States as well, such as The Netherlands and the UK. Moreover, at the time this report was finalized, the Article 29 Working Party was considering the possibility of approving BCRs on a pan-European basis, though it is likely this would not replace the necessity of having such BCRs approved at the national level as well.

4 Drafting and implementing binding corporate rules

Drafting binding corporate rules

Tailoring the rules to business needs

The BCRs need to be drafted to meet specific legal requirements. Some DPAs have published guidance on the drafting of BCRs. For example, the U.K. Information Commissioner and Austrian DPA have recently published guidelines clarifying the issues a company must address in its BCRs.[30]

BCRs will be more effective if they are uniquely tailored to fit the company's needs and culture. The U.K. Information Commissioner notes that BCRs should be more that a simple restatement of the U.K. Data Protection Act – instead they should include added value such as practical guidance to staff on how to achieve compliance in specific situations.[31] Additionally, uniquely tailored rules show an intent to comply with the law rather than the "empty formalism" conveyed by a boilerplate code.

Selecting a team to draft the rules

As BCRs affect many aspects of the operation of a company, they should be prepared by a team of relevant employees. Legal counsel, ideally expert in the area of data protection, should be involved to ensure the BCRs meet the relevant legal requirements. Managers are needed to analyze practical implementation and enforcement issues such as self-audits. Employee representatives may also need to be involved or consulted as BCRs will likely impose duties on existing employees. For example, it is necessary to ensure that adoption of the BCRs will not contravene existing contractual and legal rights of employees. Finally, communications or public relations staff may help write and present the BCRs so that they can be understood by employees, supervisors, data subjects, and DPAs.

The substance of the binding corporate rules

The substance of binding corporate rules will depend on many factors, including the needs of the corporate group using them, the type of data it is processing and the purposes of processing, the applicable legal requirements, and so on. There is no need for a standard form of BCRs, and it can be expected that they will differ between the geographic regions, legal systems, and business sectors in which they are used.

Nevertheless, there are a number of elements common to different BCRs. The most extensive analysis of the substance of BCRs so far has been provided by the EU's Article 29 Working Party (comprised of all the EU DPAs) in its Working Paper 74.[32] These

[30] "Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers: Putting the concept into practice in the United Kingdom", Information Commissioner, Feb. 11, 2004.

[31] "Required Contents of a Submission for Approval of 'Binding Corporate Rules' to the Information Commissioner", Information Commissioner, SR/HC/BCR Checklist 11/2/2004, page 1.

[32] Working Document (WP74) adopted by the Article 29 Working Party on June 3, 2003 on "Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers".

requirements are examined here for illustrative purposes only; there is no suggestion that they should be applied uniformly in all jurisdictions around the world.

Describe processing and flows of information

The BCRs must explain the transfers being authorized in a level of detail sufficient to allow the DPA to assess whether the protection being given to the data in the third countries is adequate. The Working Party suggests that the BCRs include a detailed description of the economic activities pursued by the different entities of the corporate group. In countries where the legislation creates a notification system requiring a high level of detail of pending transactions, the BCRs should mirror the level of detail in their description of the processing and flows of information.

Describe data protection safeguards

The BCRs must contain a clear description of data protection safeguards that ensure: transparency and fairness to data subjects, purpose limitation, data quality, and security, individual right of access, rectification, and objection to processing, and restrictions on onward transfers. The Working Party stresses that "the transparency of the code is a crucial element; in particular, the code should be drafted in plain language and offer concrete examples, which illustrate its provisions".[33] In practice, satisfying the transparency requirement means making data subjects aware that their personal data is being transferred to a corporate group outside of the EU using a set of BCRs approved by the DPA.

Develop a mechanism for reporting and recording changes

The Working Party and U.K. Informational Commissioner both require a company to have a mechanism for reporting changes to the BCRs to other parts of the organization and to the DPA.[34] The Working Party recommends that the company notify the relevant DPA annually with a brief explanation of the reasons justifying the changes to the BCRs.

Put in place internal measures for ensuring compliance within the organization

To ensure internal compliance, the BCRs must explain how the rules will be made known, understood, and applied effectively throughout the corporate group. For example, this should include providing employees with appropriate training and having relevant information available to them. Also, appropriate staff should be appointed to oversee and ensure compliance. The BCRs should also contain appropriate sanctions for violations, or a rigorous system of external verification, such as a requirement for external audits at regular intervals to ensure a good level of compliance.

Verify compliance

The Working Party requires that a company verify its compliance through either internal or external (or combination) audits on a regular basis by accredited auditors. The company must provide the DPA with copies of the audits and allow it (or an independent auditor on the DPA's behalf) to perform an audit on the company. While in the UK no mandatory requirement exists for providing the results of audits, the UK Information Commissioner suggests that auditing for data protection compliance be integrated with other statutorily required audits such as those required in the financial services sector.

---

[33] *Id.*, pg 11.

[34] *See, e.g.* "Required Contents of a Submission for Approval of 'Binding Corporate Rules' to the Information Commissioner" Information Commissioner, SR/HC/BCR Checklist 11/2/2004, page 5.

Develop a system to handle complaints

The BCRs must also create a system to handle complaints from data subjects. First, the BCRs must clearly identify a department or point in the organization to handle complaints. This function must be sufficiently independent of the data controllers and processors. Second, the BCRs must require the organization to provide support for data subjects making a complaint. Finally, the BCRs must provide for an easily accessible, impartial, and independent body to hear complaints from data subjects and adjudicate breaches.[35]

Affirm the duty of cooperation with the DPA

The Working Party has stressed that companies must accept a duty of cooperation with DPAs. First, both the corporate group as a whole and all of its members must agree to cooperate with the audit requirements discussed above. Second, the company must unambiguously agree to abide by the advice of the relevant DPA.

This requirement may be problematic for companies as there is likely to be confusion and uncertainty regarding the status of "advice" from the DPA.[36] Moreover, it may put a company in the position of having to reveal confidential information in conflict with local laws. It is therefore advisable for companies to delineate clear duties of cooperation with their DPAs rather than agreeing to broad, general duties.

Accept jurisdiction

The Working Party requires companies to allow data subjects to file a claim against the corporate group in either the jurisdiction of the member that is at the origin of the transfer or in the jurisdiction of the European headquarters of the corporate group. If no headquarters exists, the company must submit to the jurisdiction of the European member with the delegated data protection responsibilities.

Assure redress for individuals

The BCRs must provide for mechanisms to compensate individuals who are adversely affected by violations of them. This includes paying compensation for violations by members of the corporate group outside of the EU. Both the UK Information Commissioner and Working Party require that a company demonstrate that it has "made appropriate arrangements" to ensure the payment of compensation for any damages resulting from a breach of the BCRs. For example, the company should produce evidence demonstrating that it has sufficient assets in the Community to cover breaches of the BCRs or demonstrate that it has insurance coverage for such liability.

Accepting liability

In the EU, either the company headquarters (if the company is EU-based) or the European member with delegated data protection responsibilities must accept responsibility for the actions of other members of the corporate group outside of the Community. When a member of the corporate group in a third country has allegedly

---

[35] *Id.*

[36] "ICC comments on Working Document: Transfers of personal data to third countries: Apply Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers," International Chamber of Commerce, Commission on E-Business, IT and Telecoms, 3 Oct. 2003, page 3.

violated the rules, it is up to the company to demonstrate that the member in the third country did not violate the rules.

Promote awareness of corporate rules

The Working Party requires that the rules include provisions to ensure that information about them is readily available to any data subject who is affected by the transfer of their personal data. The UK Information Commissioner suggests that this includes providing a free copy of a company's BCRs to any data subject on their request.

Approval of binding corporate rules

The question of whether BCRs require regulatory approval is a matter for applicable law. In the EU, most but not all Member States require regulatory approval. For instance, in the UK, a company does not have to formally submit BCRs to the Information Commissioner but if it wishes to obtain approval, it must submit to the Commissioner a concise background paper explaining how the elements of WP74 have been satisfied, the BCRs themselves, and contact details of the responsible person in the organization.[37]

By contrast, in Austria approval of the DPA is required, and the application must contain at least:

1) the identity of the applicant;
2) the identities of the other group members who may become data importers, and
3) the applicant's legal enforcement capabilities as headquarters of the group against the affiliates.

The application must also contain two annexes: the substantive internal data protection rules that are mandatory within the group of companies, and the unilateral declarations of obligations regarding the data subject made by the data exporter and importers (for the purpose of illustration, English versions of these annexes are reproduced as Appendices B, C, and D). In early 2004, the Austrian DPA approved a set of corporate BCRs for the first time.

Different legal instruments can be used to make the BCRs binding both internally and externally, but not every country recognizes each legal instrument. Separate approvals in various countries may therefore be necessary.

---

[37] "Required Contents of a Submission for Approval of 'Binding Corporate Rules' to the Information Commissioner" Information Commissioner, SR/HC/BCR Checklist 11/2/2004, page 2.

5 Making the rules binding: the ICC survey

Data protection authorities have stressed that is equally important that BCRs be binding in practice as well as in law.[38] This section discusses how to make BCRs legally binding on the various entities involved in transfers of personal data.

To be binding in practice, members of the corporate group, employees, and subcontractors need to feel compelled to comply with the internal rules. While ways to ensure internal compliance may vary greatly from company to company, measures that promote compliance include:

- informational and training sessions on the BCRs for employees and subcontractors;
- disciplinary sanctions for employees who violate the rules;
- a robust complaint handling system;
- comprehensive self-audit procedures;
- appropriate redress for violation of BCRs;
- a way for data subjects to bring concerns to the relevant DPA; and
- the appointment of a Chief Privacy Officer and local privacy officers.

To be binding in law, BCRs must result in obligations that are legally binding on the companies and that can be legally enforced by data subjects and regulatory authorities. The legally binding effect of BCRs thus differs among countries and legal systems.

To learn more about the legal enforceability of BCRs around the world, ICC carried out a survey of companies in early 2004 on enforceability in different jurisdictions. Eighteen responses were received, and respondents included: US, UK, Spanish, Swiss, Danish, Belgian, and Hong Kong law firms, and Swiss, Dutch, German, Japanese, and US manufacturing companies and financial services companies. The responses show that there is a wide variety of legal principles that may lead to legal enforceability of BCRs, and that BCRs are therefore a feasible way to provide a legal basis for data transfers in many jurisdictions around the world.

DPAs generally require that BCRs are legally both:

- binding internally (within the organization), and
- binding externally for the benefit of the subject of the data.

The responses to the ICC survey are structured to respond to these two sets of requirements. In the questions below, "Yes"/"No" denotes whether the described structure would be legally binding in that jurisdiction.

Binding internally (within the organization)

To be binding in law within the organization, the rules must be:

1. binding within the corporate group,
2. binding on employees, and
3. binding on subcontractors.

[38] Working Document (WP74) adopted by the Article 29 Working Party on June 3, 2003 on "Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers", page 10.

1 Binding within the corporate group

There are many possible ways to make a set of BCRs binding on all members of a corporate group. The applicability of legal devices varies from one jurisdiction to another.

(a) Agreements involving contracts

Across the jurisdictions, respondents stated that agreements involving contracts would clearly make the BCRs internally binding.

(i) A code of conduct backed by intra-group agreements either with each member of the organization or each member having separate identical contracts with the parent company

Belgian firm	Yes	
Danish firm	Yes	
German firms	Yes	
Dutch firm	Yes	
Spanish firm	Yes	It must be clearly stated as an obligation, rather than a code of practice.
British firms	Yes	
Japanese firm	Yes	
Hong Kong firm	Yes	
Swiss firms	Yes	
US firm	Yes	

(ii) Acceptance of responsibility by contract with other group companies for the acts of other group members worldwide

Belgian firm	Yes	
Danish firm	Yes	
German firms	Yes	
Dutch firm	Yes	
Spanish firm	Yes	
British firms	Yes	
Japanese firm	Unclear	
Hong Kong firm	Yes	
Swiss firms	Possible	Possible conflicts with shareholder interests and local laws. Also, lack of clear beneficiary is problematic.
US firm	Yes	

(iii) Contracts backed by internal memo
There would be a contract between one EU company (to accept liability for all EEA members) and one non-EEA company (to accept liability for all non-EEA members). These two individual companies would contract for and on behalf of all the other companies in the group. Those other companies would confirm the arrangements by internal letters / memos.

Belgian firm	Yes	
Danish firm	Possible	Not binding if they are separate legal entities.
German firms	Yes	
Dutch firm	Yes	
Spanish firm	Yes	
British firms	Yes	
Japanese firm	No	
Hong Kong firm	Yes	
Swiss firms	Possible	Binding if the internal document is a lawful power of attorney.
US firm	Yes	

(b) Agreements involving unilateral undertakings

Unilateral undertakings are not recognized at all in some countries. In others, the law is unclear. In countries that recognize unilateral undertakings, respondents agreed that the most attractive approach for international organizations seeking approval of BCRs would be unilateral declarations. For example, in the UK the most attractive option for companies would likely be the Deed Poll.

(i) A unilateral undertaking (such as a Deed Poll)
A Deed Poll is a unilateral deed containing undertakings by an English entity to an ascertainable body or person to perform certain obligations. These are called a "speciality" – a contract under seal. No consideration passes to the giver of the undertakings, but the UK has a legal mechanism that the execution of such a document as a Deed creates valid consideration. Such a structure is binding on the entity executing the Deed under English law, and is enforceable by those in whose favor the undertaking is given. An example of such a structure is contained in the UK Telecommunications Ombudsman's Scheme, where members of the Scheme execute a deed poll in favor of individuals who might suffer loss as a result of their activities, who can enforce the undertakings given.[39]

Austrian civil law also recognizes the legal enforceability of a unilateral undertaking (called an *Auslobung*); such a unilateral undertaking was the legal basis for approval by the Austrian Data Protection Commissioner of a set of BCRs of an Austrian bank in early 2004.

[39] This document can be viewed at http://www.otelo.org.uk/resources/documents/TOSL%20Deed%20Poll.pdf.

Belgian firm	Yes	
Danish firm	Yes	
German firms	Yes	But need approval from all regional DPAs in Germany.
Dutch firm	Yes	Headquarters needs to declare that data subject can file claim in Netherlands if the data subject's country does not recognize the binding nature of a unilateral declaration.
Spanish firm	No	
British firms	Yes	
Japanese firm	No	
Hong Kong firm	Yes	
Swiss firm	Possible	Similar device ("letter of comfort") might achieve same result.
US firm	Possible	Unilateral declarations aren't recognized but, FTC might prosecute breach of unilateral declaration as an unfair / deceptive trade practice.

(ii) A unilateral undertaking by way of a Declaration of Trust

A Declaration of Trust is a unilateral declaration by the creator of the trust in favor of a defined group of persons. Presumably, those persons will be the data subjects. The stated object of the trust would be to recompense claimants who have suffered loss or damage. In order to ensure that there is an EU entity responsible for loss or damage caused by its affiliates outside the EU and able to meet those obligations, they would place assets in a trust with an EU group company in a jurisdiction that recognizes the concept of a trust. The trustee would be given the duty of paying out trust funds to appropriate claimants with valid claims for damages. The individual companies would not be able to wait for the return of their assets unless the trust ceased.

Belgian firm	Yes	
Danish firm	Yes	
German firms	No	German law does not recognize trust, but could reach similar solution through third party beneficiary contracts between involved companies.
Dutch firm	Unclear	
Spanish firm	No	Spanish law does not recognize trust, but similar devices under Spanish law.
British firms	Yes	
Japanese firm	No	
Hong Kong firm	Yes	
Swiss firms	Possible	Swiss law does not recognize trust, but equivalent devices exist.
US firm	Yes	

(iii) A unilateral undertaking or contract incorporating other regulatory issues
The entities in question within a group of companies would agree or undertake to each other (or each would undertake to all others) to follow obligations set out in statutory codes within a defined legal framework, such as the listing requirements of the local Stock Exchange or other industry codes. However, one problem with this option is that companies are likely to oppose incorporating additional government involvement with their corporate governance.

Belgian firm	Yes	
Danish firm	Yes	
German firms	Yes	
Dutch firm	Yes	
Spanish firm	Yes	
British firms	Yes	
Japanese firm	Yes	
Hong Kong firm	Yes	
Swiss firms	Possible	Possible conflicts with shareholder interests and local laws.
US firm	Possible	Needs to be adequate consideration or reliance to be binding.

(iv) Acceptance of responsibility by unilateral undertaking for the acts of other group members worldwide

Belgian firm	Yes	No trust in Belgium, but equivalent structures may exist.
Danish firm	Yes	
German firms	No	
Dutch firm	Yes	
Spanish firm	Yes	
British firms	Yes	
Japanese firm	Unclear	
Hong Kong firm	Yes	
Swiss firms	Possible	Possible conflicts with shareholder interests and local laws.
US firm	Possible	Unilateral promise usually not enforceable unless reliance.

Additional issues for unilateral undertakings

To make a unilateral undertaking work, is it necessary to have to have letters of agreement or some type of contractual commitment so that the company giving the undertaking has recourse to the other group of companies if it pays for the misuse of personal data by other members of the group?

Belgian firm	Yes	
Danish firm	Yes	
German firms	No	
Dutch firm	Unclear	
Spanish firm	Yes	
British firms	No	Not necessary, but it would “clearly be wise” to agree to some type of reimbursement mechanism.
Japanese firm	Unclear	
Hong Kong firm	No	
Swiss firms	Unclear	Undertaking must be by parent company, and possible conflicts with shareholder interests and local laws.
US firm	Yes	But, unilateral undertakings are generally not enforceable.

Can individuals bring successful claims against one member of a group of companies where the loss or damage has been caused by another?

Belgian firm	No	
Danish firm	No	
German firms	Possible	Needs to be a contract / guarantee between the companies.
Dutch firm	Yes	
Spanish firm	No	
British firm	Yes	Where the dependent company has committed to provide compliance or assumed a supervisory responsibility over the other company.
Japanese firm	No	
Hong Kong firm	No	
Swiss firms	Possible	Liability of the holding company according to "Konzernvertrauen" could lead to claims for a loss / damage caused by a group company.
US firm	Yes	

(c) Other possible structures

In the UK, another possible legally binding structure is for the parent company to unilaterally declare that it assumes a duty of care over personal data processed by itself and its subsidiaries. Any breach of that duty of care would entitle a data subject to bring a claim in "negligence" under English law. Establishing such voluntary duties used to be impractical, but this is no longer the case since *White v Jones* [1995 2 SC 207].

In the United States, two other possible structures exist. First, a self-regulatory body could be created, and contractually given enforcement power by its members, e.g. a professional association. Second, the U.S. Federal Trade Commission has asserted broad authority over enforcement of unfair or deceptive trade practices. This enforcement authority might be applied to violations of corporate rules - at least to the extent US consumers are affected

2 Binding on employees

(a) By way of specific obligations in an employment contract

Belgian firm	Yes
Danish firm	Yes
German firms	Yes
Dutch firm	Yes
Spanish firm	Yes
British firms	Yes
Japanese firm	Yes
Hong Kong firm	Yes
Swiss firms	Yes
US firm	Yes

(b) By linking observance of the rules / code of conduct with disciplinary procedures.
While all respondents agreed that linking employees' observance of the rules with disciplinary procedures would improve compliance with the BCRs, some cautioned that such actions would not make the BCRs legally binding on employees. Also, a minority of respondents were concerned that, in practice, disciplinary procedures can be difficult to enforce against employees.[40] To supplement disciplinary procedures, the U.K. Information Commissioner has suggested arranging adequate training programs and providing evidence of senior staff commitment to the BCRs.[41]

Belgian firm	Yes
Danish firm	Yes
German firms	Yes
Dutch firm	Yes
Spanish firm	Yes
British firms	Yes
Japanese firm	Yes
Hong Kong firm	Yes
Swiss firms	Yes
US firm	Yes

3 Binding on Subcontractors

All respondents were unanimous in agreeing that BCRs could be made binding on subcontractors by including relevant compliance clauses in subcontracts. However, in practice the subcontractor usually does not need to be bound by the BCRs because most subcontractors are data processors. Data processors, unlike data controllers, only need to make adequate security arrangements for the protection of the personal data. Normally, a company can ensure that a subcontractor will make adequate security arrangements through use of the Model Contracts. Thus, even if a company has a set of BCRs in place, it will likely continue to use Model Contracts when working with subcontractors.

Belgian firm	Yes
Danish firm	Yes
German firms	Yes
Dutch firm	Yes
Spanish firm	Yes
British firm	Yes
Japanese firm	Yes
Hong Kong firm	Yes
Swiss firms	Yes
US firm	Yes

[40] In particular, Swiss, Spanish, and UK lawyers were concerned with this issue. *Id.*

[41] "Required Contents of a Submission for Approval of 'Binding Corporate Rules' to the Information Commissioner" Information Commissioner, SR/HC/BCR Checklist 11/2/2004, page 3.

Binding externally (for data subjects)

WP74 requires that individuals, the relevant data subjects, be able to enforce the rules / codes via the national regulator of the data subject or the national courts. Claims must be capable of being brought and enforced by individuals against the group company in the EU member of a group which validly agrees to take responsibility for data protection breaches by other group members outside the EU.

There are two principle methods to making the rules binding externally for data subjects: unilateral undertakings and contracts.

1 Unilateral undertakings

(a) Unilateral declarations by the parent company

Belgian firm	Yes	
Danish firm	Yes	
German firms	Yes	But may need approval by all German DPAs.
Dutch firm	Yes	Headquarters needs to declare that data subject can file claim in Netherlands if the data subject's country does not recognize the binding nature of a unilateral declaration.
Spanish firm	No	
British firms	Yes	Deed Poll is likely the preferred method.
Japanese firm	No	
Hong Kong firm	Yes	
Swiss firms	Possible	Possible through use of "letter of comfort".
US firm	Possible	Unilateral declarations aren't recognized but, FTC might prosecute breach of unilateral declaration as an unfair / deceptive trade practice.

(b) Declaration of trust in favor of data subjects:
According to our respondents, a trust mechanism could be legally binding on the trustee (the relevant group company in the European Economic Area with group data protection responsibility) and enforceable by the beneficiaries against it in some EU jurisdictions. However, in jurisdictions where the use of trusts would be binding, trusts were viewed as an unattractive option compared to unilateral declarations, especially for tax purposes.

Belgian firm	Yes	
Danish firm	Yes	
German firms	No	German law doesn't recognize trusts.
Dutch firms	Unclear	
Spanish firm	No	Spanish law doesn't recognize trusts.
British firms	Yes	
Japanese firm	Unclear	
Hong Kong firm	Yes	
Swiss firms	No	Swiss law doesn't recognize trusts.
US firm	Yes	

2 Contracts

The second device to make the BCRs externally binding for data subjects is to have the data subjects be third party beneficiaries of contracts. This could be achieved through two types of contracts:

(a) contracts between the various corporate groups in which the data subjects are third party beneficiaries;
(b) a contract between the parent company and the DPA in which the data subjects are third party beneficiaries.

According to the Working Party, all EU member countries have legal devices equivalent to third party beneficiary contracts.[42] Similarly, respondents to our survey agreed that the rules could be made externally binding for a data subject by use of their national equivalent of a third party beneficiary contract.

Belgian firm	Yes	By using a commitment for third person ("stipulation pour autrui").
Danish firm	Yes	But, cannot force data subject to put make claim.
German firms	Yes	By using a third party beneficiary contract ("Vertrag zu Gunsten Dritter").
Dutch firm	Yes	By publishing the code of conduct, or third party beneficiary contract.
Spanish firm	Yes	Liable to subject under Data Protection Act if company acts contrary to the law.
British firms	Yes	Under Contracts (Rights of Third Parties) Act.
Japanese firm	No	
Hong Kong firm	No	No equivalent device to third party beneficiary contracts in Hong Kong.
Swiss firms	Yes	By using a contract in favor of a third person (art. 112 section 2 of Swiss Code of Obligations).
US firm	Possible	In certain sectors (health and financial services) there are statutory privacy obligations. In other sectors, liability would require a showing of violation of a duty of care, or reliance by the third parties.

About ICC

ICC is the world business organization, the only representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world. ICC promotes an open international trade and investment system and the market economy. Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment, e-business, IT and telecoms policy, as well as on vital technical and sectoral subjects. ICC was founded in 1919 and today it groups thousands of member companies and associations from over 130 countries.

[42] Working Document (WP74) adopted by the Article 29 Working Party on June 3, 2003 on "Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers", page 12, footnote 10.

6 Appendices

APPENDIX A:

Codes of conduct and their binding nature

Name of Code	Organisation	Derived from	Voluntary	Legally enforceable	Membership based?	Enforceable by
Bank certification network for financial and e-commerce transactions	Identrus formed by ABN AMRO, Bank of America, Deutsche Bank, Barclays, JP Morgan Chase, Citigroup and Hypovereinsbank	Identrus defined policies for technology, risk management, contracts and business practices	Y	Y	Y	Identrus through system rules
BBB Code of Advertising	Better Business Bureau "BBB"		Y	N	Y	Council of BBB
British Columbia Shellfish Aquaculture Code of Practice	The Ministry of Agriculture, Food and Fisheries	Related Legislation	N	Y	Y	The Ministry of Agriculture, Food and Fisheries
British Standard BS6853 - "Code of Practice for fire precautions in the design and construction of passenger carrying trains"	British Standards		Y		Y	
BS7799 or ISO 17799	British Standards		Y		N	
Business Banking Code	The British Bankers' Association (BBA), the Building Societies Association and the Association for Payment Clearing services		Y	BCSB hears complaints. Consumers can go to the Financial Ombudsmen Service who will take the codes into account when decision making. The Ombudsmen's decisions are binding on parties	Y	Monitored by the Banking Code Standards Board (BCSB)
CAP Code	Committee of Advertising Practice & Advertising Standards Authority	Legislation (long list)	Y	N, but ASA can refer matter to Office of Fair Trading to take action under Control of Misleading Advertisements Regulations (CMARs)	Y, but can also apply through contract	CAP
Cloud Cover	CESG (root authority which certifies CSPs for the government), a part of the UK Civil Service		Yes Mandatory for UK Government			UK Accreditation Service

Name of Code	Organisation	Derived from	Voluntary	Legally enforceable	Membership based?	Enforceable by
Code of Conduct and of Practice	British Computer Society	Code of Practice by Royal Charter	Y	N	N, the Code of conduct applies as long as the firm is offering expertise as part of the Society's Professional Advice Register HOWEVER the Code of Practice is solely for members	BCS
Code of Conduct and Professional	Association for Computing Machinery				Y	
Code of Practice to promote high standards within the computer and electronic games industry	The Video Standards Council	The Video Standards Council in consultation with the industry members established the rules	Y	N	Y	N
Codes of Conduct	Swiss Bankers' Assc	Article 11 of The Stock Exchange Act 1997	Y	Y, the Rules of Conduct for Securities Dealers in the Performance of Securities Trading Operations ("SBA-Rules of Conduct") are legally enforceable ((1997) 10 JIBFL 479 "Switzerland New Rules of Conduct for Security Dealers")	Y	Federal Banking Commission (SBA's regulatory authority)
Codes of Practice: Advertising, age rating	Entertainment and Leisure Software Publishers Association		Y		Y	Advertising Code: The Advertising Standard Authority
D.M. Code of Conduct	Direct Marketing Assc	Marketing Legislation	Y	N, but can in its Annual Report indicate breaches by a corporation to the Director General of Fair Trading and can also report to the Office of Fair Trading	Y	Direct Marketing Authority
E-Terms 2004	International Chamber of Commerce		Y			
European Union Standardisation Initiative	European Union					ETSI/CEN

Name of Code	Organisation	Derived from	Voluntary	Legally enforceable	Membership based?	Enforceable by
Forty Recommendations [and Eight Special Recommendations]	Financial Action Task Force	Organisation a result of G7 Summit in Paris 1989. Recommendations developed in 1990 [also within the Recommendations, are references to various UN Conventions]	Y	N, but members expected to implement the Recommendations through national law, regulations or administrative practice.	Y, but designed for universal application.	FATF, can blacklist countries disabling them to do financial business with other members
French Electronic Signatures		Based on International Standards: ISO 9000, BS 7799	Y	Y		French Accreditation Body (COFRAC)
Gap Clothing - Sourcing Code	Gap	_	Y	Yes through private contracts	Yes have to have contract with Gap	GAP and some third parties
General Insurance Information Privacy Code- This was approved by the Information Commissioner as an alternative to the relevant legislation	Insurance Council of Australia	Privacy Act 1988	Y	Y	Y	Independent Adjudicator: The Privacy Compliance Committee (PCC) and a Committee of Insurance Enquiries and Complaints. Determination of the PCC is enforceable through the federal court or the federal magistrates court.
GISE Commercial Codes, GISE Private Codes	General Insurance Standards Council		Y	N	Y	Financial Ombudsman Service or the GISC Dispute Resolution Facility (DRF)
GUIDEC	International Chamber of Commerce					ICC Information Security Working Party
ICA Code of Ethics	International Compliance Assc		Y	N	Y	ICA
IEC 60364	International Electrotechnical Commission	Harmonisation of Existing Rules in Europe				

Name of Code	Organisation	Derived from	Voluntary	Legally enforceable	Membership based?	Enforceable by
INCOTERMS	International Chamber of Commerce	INCOTERMS 2000	Y	Y	N	Must be incorporated into contract
Industry environmental codes; Environmental Compliance Codes, Nature Conservation Codes	Environment Protection Agency	Environmental Protection Act 1994	Y	N	N	
Investor in People Quality Standard	Investor in People	The Standard was developed during 1990 by the National Training Task Force in partnership with leading national businesses	Y	Does not appear to be the case. Reviews are held instead- not more than three years apart.	Y	Investors in People
ISIS (Industrial Signature Interoperability Specification)			Y			
Model International Law on E-commerce			Y		Y through United Nations Membership	United Nations Commission on International Trade Law
Mutual Recognition Arrangements	ViTAS	ViTAS (D02) V0-01A Code of Practice and ViTAS (D04) A Management Structure and Processes	Y		Y	ViTAS
NEC	National Electrical Code	Based on North American Principles and Practice over 100 years		Y		Verification Bodies
No rules; it campaigns for legislation	Consumers' Assc; "Which?"	N/A	Y	N	Y	N/A
Number of Codes for the elimination of various types of discrimination in the Employment sector	Equal Opportunities Commission	The Commission is empowered to issue codes according to the Sex Discrimination Act 1975	Y	The codes are admissible in court	Y	The commission and the involved Parties
Quality Code for Wool Fabrics	International Wool Textile Organisation		Y		Y	
Safe Harbor	U.S. Department of Commerce and the European Commission	EU Data Protection Directive	Y	Y	N	Federal Trade Commission

Name of Code	Organisation	Derived from	Voluntary	Legally enforceable	Membership based?	Enforceable by
T - Scheme	T-Scheme	ETSSI Standards, Electronic Communications Act, Directive 1999/93	Y			Self Regulation
The Canadian Care Labeling Code	Competition Bureau. This is part of Industry Canada	The federal government initiated the standard and the garment industry voluntarily applies it.	Y	N	N	Competition Bureau
The Guide to the Professional Conduct of Solicitors	The Law Society of England and Wales	Solicitors Practice Rules 1990	N compulsor y	Y	Y	The Law Society of England and Wales
There are currently five Maritime and Coastguard Agency codes applied to small vessels in commercial use	Maritime and Coastguard Agency	Merchant Shipping (Vessels in Commercial Use for Sport or Pleasure) Regulations 1998	Y	Y	N	Maritime and Coastguard Agency
UCP 500	International Chamber of Commerce		Y		N	
Voluntary Code of Practice for the Security of Dangerous Goods by Roads	Department for Transport	This Code builds on the principles set down in the United Nations	Y		Y	
Voluntary Codes in the Financial Sector	Financial Consumer Agency of Canada	Derived from consulting with the financial industry	Y	N	N	Complaints heard by FCAC
Wolfsberg AML Principles	The Wolfsberg Group		Y	N	N, can be adopted by any bank	

APPENDIX B

Mandatory Internal Data Protection Rules for BCRs under Austrian Law*

SAMPLE INTERNAL DATA PROTECTION RULES:

Members of the group established in third countries shall comply with the following provisions of the Austrian Data Protection Act 2000, published in Fed. Law Gazette part I Nr. 165/1 999:

– Article 2 sections 1, 2 (with the exception of §§ 5, 12 and 13) 3, 5, 8 and 9; moreover § 58 concerning data processing in manual files.

In addition, each group member established in a third country shall process personal data imported from other group members established in the EU in accordance with the following rules:

a) in case of onward transfers of data to a controller who is not bound by these data protection rules or has not chosen to subject to these rules for this case of onward transfer, to give the data subject the opportunity to object, or, in case of transfer of special categories of data, to carry out the transfer only if the data subject has given his or her unambiguous consent;
b) to inform headquarters immediately if the country in which the member is established introduces legal provisions or factual procedures likely to make it impossible to comply with essential parts of the above mentioned data protection provisions;
c) in case of queries or demands for access by data subjects concerning data which have been imported from an EU member state, to inform headquarters without unnecessary delay about the fact and the answers given or measures taken;
d) to designate a body or person in charge of data protection questions within the company, to establish a procedure for dealing with complaints by data subjects, and to provide accurate information concerning these facts to headquarters at any time;
e) to provide for regular adequate control measures concerning compliance with the substantive data protection rules; and
f) to inform headquarters without unnecessary delay about all occurrences relevant for data protection, especially about complaints by data subjects, and to use its best efforts to support data protection audits conducted on the demand of headquarters.

* Unofficial translation by Christopher Kuner.

APPENDIX C

Unilateral declaration of obligations vis a vis the data subject made by the data exporter under Austrian law**

SAMPLE UNILATERAL DECLARATION: by the Data Exporter:

The company, as the headquarters of the group of companies consisting of the group members listed in Annex 1, declares publicly for the benefit of all persons whose personal data will be processed in Austria by one of the group members in its function as a controller in the case of an export of such data from Austria to a group member established in a third country not affording adequate data protection as defined in Directive 95/46/E to honour the following obligations:

1. to guarantee that the group members in third countries comply with the substantive data protection rules set out in Annex 3 when processing such personal data;

2. to forward these mandatory data protection rules to the Data Protection Register in order to make them available to the data subjects; (can be deleted, if the substantial rules are the national DP-law of the exporting country);

3. to see to it that queries and requests for access made by data subjects to headquarters or foreign group members concerning the processing of their data after transfer within the group are answered correctly, completely and without unnecessary delay;

4. in case of a future revocation of this declaration, to continue to comply with the obligations of this declaration concerning those data which were transferred before revocation and have not yet been deleted; and

5. to acknowledge that any disputes arising from this declaration shall be settled before a competent court in Vienna, Austria, Austrian law being the applicable law in such procedure.

** Unofficial translation by Christopher Kuner.

APPENDIX D

Unilateral declaration of obligations vis a vis the data subject made by the data importer under Austrian law[***]

SAMPLE UNILATERAL DECLARATION: by the Data Importers:

Each of the signatory affiliate group members established in a third country not affording adequate data protection as defined in Directive 95/46/EC declares per se publicly for the benefit of all persons whose personal data are processed in Austria by one of the group members in its function as a controller to honour, having imported their data from Austria, the following obligations:

1. to follow the substantial data protection rules set out in Annex 3 when processing personal data and to be liable for damage resulting from such processing according to § 33 öDSG 2000;

2. to answer queries and requests for access brought forward by data subjects concerning the processing of their data within the group, correctly, completely and without unnecessary delay;

3. in cases where the data subject approaches the Austrian DPA in a procedure according to § 30 DSG 2000 concerning data falling under the present declaration, to take part in this procedure as the claimants adversary;

4. in case of a future revocation of this declaration, to continue to comply with the obligations of this declaration concerning those data which were imported before revocation and have not yet been deleted; and

5. to acknowledge that any disputes arising from this declaration shall be settled before a competent court in Vienna, Austria, Austrian law being the applicable law in this procedure.

[***] Unofficial translation by Christopher Kuner.