Binding corporate rules – a pan-European perspective

The development of binding corporate rules as a mechanism to ensure adequacy of protection for international data transfers is a welcome solution for multinationals seeking to reduce the administrative burden associated with data protection law. **Simmons & Simmons**' European Information and the Law Group looks at the approach being taken in various European jurisdictions to binding corporate rules.

On June 3rd 2003 the Working Party of the EU Data Protection Commissioners (the "Article 29 Working Party") adopted a working document aimed at providing a mechanism whereby a multinational company or group of companies may transfer personal data throughout its organisation without being required to, for example, enter into a complex web of intra-group contracts based on the European Commission model contracts. Clearly, however, the Article 29 Working Party would not sanction the use of corporate policies to cover intra-group transfers of data unless they felt that the corporate policy adopted guaranteed similar levels of protection for individuals as is guaranteed through use of the European Commission model contracts.

One of the key features of a set of binding corporate rules is, therefore, that they are binding on each organisation within the corporate group. According to the Article 29 Working Party this means that they must be both legally enforceable and binding in practice. Consequently, not only must the group companies consider themselves bound by the rules but also the rules must give enforceable rights to the relevant data subjects. Examples of how the rules may be brought into effect include internal policies (the application of which is the responsibility of the headquarters) or internal codes backed by intra company agreements. The Article 29 Working Party believes that legally enforceable third party rights to a contract may now be put in place in all Member States and, in some instances, the introduction of binding corporate rules may be effected simply by the inclusion of an additional clause into existing intra company agreements enabling the enforcement of the policy by individuals.

The Article 29 Working Party has stressed that ensuring the legitimacy of binding corporate rules does not finish with their inclusion in a corporate handbook. Any organisation applying to have its rules accepted must notify the relevant data subjects, make provision for a complaints handling procedure, be prepared to abide by any advice from data protection authorities and accept that the bottom line is that it could be sued by the data subjects for any breaches.

The United Kingdom

The UK's Information Commissioner has clearly indicated that its approach will be based on the high level principles of the Article 29 Working Party's guidance. However, at this stage, the Information Commissioner is keen to emphasise that it does not wish to be prescriptive about the format of any binding corporate rules document, preferring to give organisations licence to use their own house style to deliver compliance while ensuring that the end product is of sufficient quality to be assessed properly (see *PL&B UK*, Feb/March 2004, p.6).

In relation to the contents of such a document, the overriding requirements highlighted by the Information Commissioner as being integral to the Article 29 Working Party's guidance are:

- the demonstration of a good level of compliance
- provision of support and help to individuals; and
- appropriate redress mechanisms.

In addition, the Information Commissioner has set out more specific content requirements (under certain key headings) which need to be included in the document, the most salient of which are summarised below.

Jurisdictions covered:

United Kingdom
France
Italy
Netherlands
Belgium
Germany

The Information Commissioner has made it clear that legal enforceability is a prerequisite of the binding corporate rules and specific mention in the rules should be made of procedure on non-compliance and legal remedies. However, the formulation of a corporate policy in such a manner as is enforceable by the individual but which does not place onerous restrictions on the business could well be difficult to achieve in practice.

The Information Commissioner also believes that organisations should set out the extent of the transfers they anticipate to be covered by the rules as well as the purposes of the processing and how these purposes relate to the organisation's business activities. In addition, measures for ensuring compliance in the day to day operation of the organisation, including staff training, as well as mechanisms for checking continued compliance (including audit requirements and step-in rights for the Information Commissioner) should be set out.

This area of data protection compliance is a new development for both data controllers and the UK Information

Commissioner alike. It would seem that the Information Commissioner is currently developing its approach in cooperation with various interested parties. Further guidance can be expected as its experience in this area grows.

FRANCE

France has not yet implemented the EU Data Protection Directive. However, a draft bill dated April 29th 2004 which is intended to implement the directive into French law is currently being discussed in Parliament and should be adopted this year.

In line with the requirements set out in the Directive, the draft bill provides that transfers to countries that do not offer an adequate level of protection may be authorised by the French Data Protection Authority (the CNIL) if there is an internal policy that can ensure an adequate level of protection for individuals' privacy and fundamental rights and freedoms.

Although the CNIL has not yet issued any express recommendations concerning the format of such internal policies, we understand that it is keen to adopt a proactive role in relation to their drafting. The CNIL has informally indicated that its two principal concerns are that:

- the internal policy is enforceable against each entity within the corporate group; and
- in practice, each entity of the corporate group has the means available to enforce it.

The CNIL is also aware of the issue concerning the enforceability of the internal policy by data subjects. While in some jurisdictions, data subjects may become third party beneficiaries through the insertion of a unilateral undertaking in the internal policy, the validity of this type of undertaking is questionable under French law. In France, it will therefore be necessary for the group to put in place appropriate contractual arrangements which allow data subjects to enforce the internal policy.

The CNIL considers that internal policies should be far more attractive and efficient in the context of a group of companies than the European Commission model contracts. It is eager to assist French-based corporate groups that are considering the implementation of such policies as an alternative to entering into a series of intra-group contracts based on the European Commission model contacts.

ITALY

The Italian legislation on data protection (Legislative Decree 196/03 "Codice in materia di protezione dei dati personali" (the Code) does not contain any provision giving intra-group binding corporate rules an official legal effect. Moreover, the Italian Data Protection Authority (the Garante) has not released any specific decision that sanctions the use of such corporate rules as an alternative to intra-group contracts for the transfer of data abroad, or that even considers the Article 29 Working Party's guidance.

Consequently, data controllers governed by Italian law are not yet able to rely on binding corporate rules to sanction the transfer of personal data outside the European Economic Area (EEA). Accordingly, data controllers will either have to use the European Commission model contracts or rely on certain exemptions in the Code (eg. transfers for the performance of obligations resulting from a contract to which the data subject is party, transfers for safeguarding a substantial public interest, transfers in response to a request for access to administrative records etc.). Alternatively, the data controller could ensure that "corporate rules" are inserted and form part of a formal contract, signed by the transferor company and the recipient company, that regulates the transfer of data. However, that contract would have to be submitted to the Garante for specific authorisation for the transfer of personal data. The Garante will check whether the contractual clauses laid down in the agreement offer adequate safeguards with respect to the protection of individuals' privacy.

THE NETHERLANDS

The Dutch Data Protection Act (Wet Bescherming Persoonsgegevens, (WBP)), which implements the Data Protection Directive, provides a number of mechanisms to transfer data overseas. Practice has shown that multinationals encounter difficulties when trying to follow the WBP's provisions governing the exchange of data within a corporate group. The Dutch Data Protection Authority (College Bescherming Persoonsgegevens, (CBP)) is aware of this problem.

The CBP recognises the use of binding corporate rules for multinationals as an alternative or complementary instrument for the transfer of data to countries not offering an adequate level of protection where resorting to the other transfer mechanisms presents too many hurdles. Since the CBP has not issued any directions in connection with the required format for such binding corporate rules, each data controller is, in principle, free to shape its own binding corporate rules as long as the principles set out in the directive and in the WBP are observed.

Some multinationals present drafts which specifically focus on the transfer of personnel data through their group, providing data subjects with adequate safeguards (for example, enforceability mechanisms) and set the principles of their data processing in human resources policies which also address other company values. Others insert the principles that will govern their privacy matters in codes of conduct especially designed to cover only data

Multinationals closer to EU-wide approval on corporate rules

In early June, a meeting in Berlin brought together national data protection authorities (including the UK, the Netherlands, Germany, France, Austria, Hungary and Poland) and a number of multinational companies (including General Electric, Philips Electronics and Daimler Chrysler) to discuss EU-wide approval of their binding corporate rules schemes.

While these companies wait for official approval of their schemes, the Article 29 Working Party is currently working on a new report which will lay out the approval criteria for the schemes. The report could be approved by the Working Party in the next few months.

protection aspects.

Our experience in this field shows that the process of obtaining approval for binding corporate rules is lengthy and marked by intensive negotiation rounds with the CBP.

Certain major multinationals are currently seeking the CBP's approval of their draft binding corporate rules. Despite positive unofficial reactions of the CBP towards these initiatives, at this stage no draft binding corporate rules have been approved. As soon as approvals are granted, it will be clearer as to what content and form is required of other multinationals wishing to adopt their own binding corporate rules.

BELGIUM

The Belgian Data Protection Act (the Act), implementing the EU directive, does not specifically refer to intra-group binding corporate rules as a legal basis for the lawful transfer of personal data to non-EEA countries.

The Act specifically refers to the data subject's unambiguous consent to the transfer, as one of the permitted transfer grounds, even in circumstances where the non-EEA country is considered as not having an adequate level of data protection.

In line with the European Commission's policy, the Belgian Data Protection Authority considers that the United States offers an adequate level of protection provided that the data recipient has accepted the "safe harbour principles".

Other permitted transfer grounds regardless of whether the non-EEA country offers an adequate level of protection, include the transfer which is necessary for the performance of a contract to which the data subject is a party, and the transfer necessary for the performance of a contract that has been or will be concluded for the benefit of the data subject without the latter being a party to that contract.

As an alternative or complementary ground for the transfer of data to a non-EEA country with an inadequate level of data protection, in circumstances where other permitted transfer grounds are not available or are too burdensome, the Act provides for the possibility of obtaining specific authorisation for the transfer.

The specific authorisation regime is where the binding corporate rules may come into play.

Under this regime, the Act requires that the data controller presents adequate safeguards with regard to privacy protection, individuals' fundamental rights and freedoms and exercise of corresponding rights. The Act specifies that these safeguards may in particular result from appropriate contractual clauses (and here the European Commission model contracts could be used).

Whether or not in contractual form, intra-group binding corporate rules may be the subject of a specific authorisation. Our experience shows, however, that this may be a lengthy process. Authorisation must obtained from the Ministry of Justice, which must first obtain the advice of the Belgian Data Protection Authority which aims to issue an opinion within two months from the request. However, there is no procedural timeframe within which the Ministry is required to give or refuse the authorisation.

GERMANY

The German regional Data Protection Authorities responsible for the private sector regularly refer to the principles of Article 29 Working Party's Guidance (see *PL&B Int*, Oct/Nov 2003, p.28). As a result, the principles relating to the situation in the United Kingdom as explained above, may be transferred to Germany as well, with respect to the content of binding corporate rules. In particular, binding corporate rules in Germany have to, inter alia, contain provisions on the principles of data processing, the purposes for which the data is processed, the categories of processed data and the rights of those affected as well as the enforceability of these rights.

However, at present there are certain grey areas, especially in relation to procedure, when dealing with binding corporate rules. The different regional German Data Protection Authorities have agreed to carry out an examination of the content of binding corporate rules submitted to them centrally within the "International Data Transmission" working committee of the so-called Düsseldorf-circle, in which all Authorities of the Federal Republic of Germany are represented.

At present, however, these Authorities have yet to make a decision as to whether single transfers or certain types of transfers of personal data into countries that do not offer an adequate level of protection must be approved. Therefore it is advisable to make early contact with the Authority responsible for the respective region (or "Land") in order to ascertain its interpretation of the law, until the various German Data Protection Authorities harmonise their approval procedures.

CONCLUSION

Looking at these jurisdictions demonstrates that most member states do have mechanisms in place allowing companies to adopt binding corporate rules. The drawback is that national authorities tend to differ in their level of commitment to the scheme and because the process is still in its infancy, those companies pioneering corporate rules can experience lengthy and laborious negotiations. Nonetheless, things are moving forward and as national authorities and businesses gain more experience, the process will likely become less complex for those planning to adopt corporate rules in the future.

AUTHORS:
United Kingdom - Alexander Brown (alexander.brown@simmons-simmons.com)
France - Patrick Martowicz (patrick.martowicz@simmons-simmons.com)
Italy - Alberto Ferrario (alberto.ferrario@simmons-simmons.com)
Netherlands - Catherine Jakimowicz (catherine.jakimowicz@simmons-simmons.com)
Belgium - frank.depaepe (frank.depaepe@simmons-simmons.com)
Germany - Berthold Hilderink (berthold.hilderink@simmons-simmons.com)