The European Journal of International Law Vol. 21 no. 2 © EJIL 2010; all rights reserved

Data Protection and Transborder Data Flow in the European and Global Context

Lingjie Kong*

Abstract

Very similar to trade barriers, data protection has been an obstacle to free global data flow. The European legal system on cross-border data flow set up by Directive 95/46/EC prohibits transfer of personal data to third countries which do not have an adequate data protection level. With enormous international implications, such a regionally oriented system is heavily dependent on effective monitoring of cross-border data transfer. Due to a lack of proper supervision on data transfer, it encounters many challenges, which forces the European Commission to adopt the contractual model and the corporate law model. Meanwhile, compared with issues like free trade and environmental protection, not much international consensus has been reached on cross-border data protection. As a result, bilateral, regional, and multilateral collaborations between national sovereignties are to be strengthened, to facilitate transborder data flow and to safeguard individuals' right to data protection.

Introduction

In the 1990s, technological innovations completely transformed sporadic cross-border data transfer, carried out through heavy data storage medias.[1] Personal data flow more freely, know fewer national attachments, and indeed represent one of the significant forces behind the processes of globalization.[2] Personal data turn into a new type of 'raw material',[3] and transborder data transfer becomes the lifeline for multinational corporations. Meanwhile, data protection is an important part of the rule

* Institute of International Studies, Wuhan University, China; SJD of Wuhan University, SJD candidate of University of Paris Sud. The author owes special thanks to Professor Philippe Achilleas (University of Paris Sud) and Professor Huang Jin (China University of Political Science and Law) for their joint supervision of my SJD dissertation, on the basis of which this article is written. Email: konglingjie80@yahoo.com.cn.

[1] OECD, *Report on the Cross-Border Enforcement of Privacy Laws* (2006), at 6, available at: www.oecd.org/dataoecd/17/43/37558845.pdf.

[2] C. Bennett and C. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2003), at 257.

[3] C. Kunner, *European Data Privacy Law and Online Business* (2003), at p. ix.

of law in the information society.[4] Due to uneven data protection levels in national sovereignties, data protection has become a major obstacle to free global data flow. As a result, the principle of free flow of information is to be reconciled with the requirements of effective data protection, regardless of frontiers.[5]

Being aware of the political and economic implications of data protection, global and regional organizations have been actively involved in coordination and harmonization of national data protection laws.[6] In particular, a strict cross-border data transfer legal system has been established by the European Union, which ensures free data flow within the community, but restricts transfer of data to third countries. Such a regionally oriented legal framework, however, faces serious challenges. As a result, standard contractual clauses and binding corporate rules on data protection in cross-border data transfer have been adopted by the European Commission. Meanwhile, the international community longs for a feasible and effective global legal framework to maintain free flow of personal data across national boundaries, and to safeguard rights of the data subjects in spite of their residence or nationalities.[7]

1 European Law on Cross-border Data Transfer

A *The CoE Convention and the Principle of Equivalence*

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention) seeks to secure in the territory of each party for every individual, whatever his nationality or residence, respect for his right to data protection. The equivalence principle is chosen as the core criterion on transborder data flow. One the one hand, obstacles to transborder data flow are not permitted between Contracting States. The rationale for such a principle is that all Contracting States, having subscribed to the common core of data protection provisions set out in the Convention, offer a certain minimum level of protection. On the other hand, transfer of personal data to non-contracting states shall be prohibited, unless equivalent protection is provided to the data being transferred.[8] Due to the fact that the number of Contracting States is limited and transfer of data to non-contracting states without equivalent data protection is prohibited, the Convention is unable keep up with the need for increasing data transfers between the Contracting States and non-contracting states.[9]

4 Blume, 'Transborder Data Flow: Is There a Solution in Sight?', 8 *Int'l J L and Info Technology* (2000) 65, at 65.

5 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention), CETS No 108, Explanatory Note, Strasbourg, 28 Jan. 1981, at para. 62.

6 Reidenberg, 'The Simplification of International Data Privacy Rules', 29 *Fordham Int'l LJ* (2006) 1128, at 1128.

7 Hondius, 'Data Law in Europe', 16 *Stanford J Int'l L* (1980) 87, at 102–104.

8 CoE Convention, *supra* note 5, Art. 12.

9 Council of Europe, Model Contract to Ensure Equivalent Protection in the Context of Transborder Data Flows with Explanatory Report (1992), Study Made Jointly by the Council of Europe, the Commission of the European Communities and International Chamber of Commerce, Strasbourg, 2 Nov. 1992, at paras 4–6.

B *Directive 95/46/EC and Cross-Border Data Transfer*

By reference to the CoE Convention, Directive 95/46/EC creates a similar legal system on cross-border data transfer. The EU system seeks to realize the dual objectives of the Directive, namely, free flow of information and effective data protection. As recitals of the Directive note, economic and social integration resulting from the establishment of the internal market lead to a substantial increase in cross-border data flow of personal data in different Member States. Meanwhile, the difference in levels of data protection in Member States may prevent transmission of personal data from one state to another. This difference may further constitute an obstacle to the pursuit of a number of economic activities at the Community level, distort competition, and impede authorities in the discharge of their responsibilities under Community law. Therefore, national laws, regulations, and administrative provisions on data protection are to be coordinated and harmonized, in order to guarantee a minimum level of data protection on the Community level.[10] The Directive formulates such a minimum level for the Member States and eliminates obstacles to transborder data flow between them.

For transfer of data to third countries, where a country is assessed by the EU as providing adequate protection for personal data, it may enjoy the same treatment as the Member States; otherwise, the data transfer is prohibited. Such a legal system, to a certain extent, builds up a firewall for personal data relating to citizens of the Union, and installs an 'iron curtain' on transfer of data outside of the Union. In consideration of the fact that the majority of third countries have not been assessed as providing adequate protection, the Directive lists six exceptional cases to the iron rule. In addition, data transferors are encouraged to provide sufficient safeguards on personal data, through which data may be transferred to third countries which do not maintain an adequate data protection level. Of course, such an approach shall be restrictively interpreted and applied.[11] In other words, adequacy in the level of data protection is the principle, while the above cases are exceptions.[12]

In summary, there are in total three legitimate grounds for transfer of data outside the European Union: (a) the destination country is qualified by the European Union as providing adequate protection of the data (Article 25(2)); (b) the data transfer belongs to the exceptional cases listed in Article 26(1); (c) sufficient safeguards are provided by measures referred to in Article 26(2).

[10] Dir. 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995, on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ (1995). 281/31, Recitals 1–9.

[11] European Commission, Data Protection Working Party, WP 12: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, DG XV D/5025/98, 24 July 1998.

[12] European Commission, Data Protection Working Party, WP 114: Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC, 2093/05/EN, 25 Nov. 2005, at 6–8.

2 The Adequacy Assessment System

A *Definition of Adequacy*

According to Directive 95/46/EC, the adequacy of the level of protection in a third country is to be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations. Particular consideration is to be given to the nature of the data, the purpose and duration of the proposed processing operation, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country, and the professional rules and security measures complied with in that country.[13] As the EU think-tank on data protection, the Article 29 Data Protection Working Party has defined adequacy and proposed criteria and means to assess it.[14]

In Europe, the tendency historically has been for data protection rules to be embodied in law, which has provided the possibility for non-compliance to be sanctioned and for individuals to be given a right to redress. Such laws have generally included additional procedural mechanisms, such as the establishment of supervisory authorities with monitoring and complaint handling functions. Outside the Union, it is still rare to find such procedural means for ensuring compliance with data protection rules. Further, data protection rules contribute to the protection of individuals only if they are followed in practice. Therefore, it is necessary to consider both contents of rules applicable to personal data transferred to a third country and systems in place to ensure the effectiveness of such rules.

Since Directive 95/46/EC sets the minimum level of data protection for the Member States, provisions of the Directive are to be the basic criteria to evaluate contents data protection rules and procedural means for ensuring data users' compliance with the data protection rules in a third country. Basic principles to be included in data protection rules shall include the purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle, the right of access, rectification, and opposition, and restrictions on onward transfers. Since there is no uniform legal enforcement pattern or model, the objectives of a data protection system are defined as: (a) to deliver a good level of compliance with the rules; (b) to provide support and help to individual data subjects; (c) to provide appropriate redress to the injured party where rules are not complied with.

B *Assessment of the Adequacy of Data Protection in Third Countries*

The Directive takes a case-study approach in assessing adequacy of data protection in third countries, which examines a specific data transfer operation or set of operations.[15] Nevertheless, given the huge number of personal data leaving

[13] Dir. 95/46/EC, *supra* note 19, Art. 25(2).

[14] European Commission, Data Protection Working Party, WP 4, WP 7, WP 9, and WP 12. Documents adopted by the Working Party are available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm.

[15] Dir. 95/46/EC, *supra* note 10, Art. 25(2).

the Union on a daily basis and the multitude of actors involved in such transfers, no Member State could ensure that each case is examined thoroughly.[16] As a result, mechanisms are to be developed to rationalize the decision-making process for a large number of cases, allowing decisions to be made timely and efficiently.

Compared with national supervisory authorities and the data transferors, the European Commission is in a better position to assess the adequacy of data protection. Such an approach is cost efficient. Member States do not have to assess the same cases, and differences between national assessments can be avoided. Furthermore, this can increase certainty and predictability for data transferors. Lastly, such an approach serves as an external push for third countries to improve their data protection.

Meanwhile, assessment of the adequacy of data protection in third countries by the European Commission faces numerous difficulties. First, third countries which have effective data protection Acts are rare. Those that follow the European model and could pass the assessment are even rarer. As a result, the guiding effect of such an approach is decreased.[17] Secondly, a few states, such as the United States, Canada, and Australia, have federal legal systems. Variations exist with regard to data protection in the states. It becomes more difficult to assess data protection in these countries. Thirdly, assessing the data protection level of a state is politically sensitive. Some third countries might see the absence of a finding that they provide adequate protection as politically provocative, or at least discriminatory.[18] In consideration of these difficulties, the European Commission takes a flexible and pragmatic approach, making only positive findings rather than negative ones. The assessment is seen as a continuing process, rather than just to produce a definite list. Countries that pass the assessment will be on the white list, which could be constantly added to and revised in the light of development. Those that do not show up on the white list are not necessarily put into the black list.

C *Shortcomings of the Adequacy Assessment System*

Up to now, countries and regions qualified as providing adequate data protection include Switzerland, Argentina, Guernsey, and the Isle of Man.[19] Positive findings are in principle limited to countries having horizontal data protection laws. They also cover specific sectors where data protection is adequate, even though in other sectors of the same country protection may be less than adequate. After assessing the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada, the European Commission deems the transfer of data to

[16] European Commission, Data Protection Working Party, WP 12, *supra* note 11, at 26.

[17] Zinser, 'European Data Protection Directive – the Determination of the Adequacy Requirement in International Data Transfers', 16 *Tulane J Technical & Intellectual Property* (2004) 176, at 176.

[18] European Commission, Data Protection Working Party, WP 12, *supra* note 11, at 27.

[19] EC Dec. 2000/518/EC, OJ (2005) L 215/1; Dec. C(2003)1731, OJ (2003) L 168/1; Dec. 2003/821/EC, OJ (2003) L 308/27; Dec. 2004/411/EC, OJ (2004) L 151/48.

Canadian transferees subject to this Act legal.[20]

Because the number of countries is limited, in practice Member States still have to assess adequacy case by case. National legislation and practice on such assessment still vary.[21] On notification and monitoring of transborder data transfer, some countries are too strict, and some are too lax.[22] In addition, the efficient operation of the adequacy assessment system is very much dependent on effective supervision of transborder data flow. No matter how perfect the system looks, in practice, data transferors may escape it. As a result, the European Commission has to shift from absolute reliance on the top-down assessment and monitoring system to a more flexible and pragmatic approach. Standard contractual clauses and binding corporate rules are two options taken by the Commission.[23]

3 The Contractual Model and Standard Contractual Clauses

Doubtless, data protection is becoming one of the top concerns for the international community. But compared with issues like transborder data flow, free trade, and environmental protection, not much consensus has been reached. Even worse, the call for data protection by some countries reflects inherent political and economic conflicts between national sovereignties. In such a context, the contractual model and the corporate law model have great potential for development.[24]

A *Development of Standard Contractual Clauses*

Transborder data flow involves the economic and political interests of states. Meanwhile, transfer of personal data from the transferor in one country to the transferee in another concerns the two parties' interests in data flow and the data subjects' right to data protection. Prior to Directive 95/46/EC, the contractual approach had already been applied by many states and international organizations to deal with relevant legal issues on data protection in cross-border data transfer.[25] By reference to existing practices, the European Commission incorporates the contractual model into its legal framework on data protection in cross-border data transfer.

As mentioned above, the principle of equivalence is the foundation of the legal system of the CoE Convention on transborder data flow. During the discussion of 'equivalent protection', being aware that some countries had already used the

[20] EC Dec. 2002/2/EC on the Adequate Protection of Personal Data Provided by the Canadian Personal Information Protection and Electronic Documents Act, OJ (2002) L 2/13.

[21] Douwe Korff, 'EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws', Study Contract ETD/2001/B5-3001/A/49, Cambridge, Sept. 2002, at 182–194.

[22] European Commission, *First Report on the Implementation of the Data Protection Directive* (2003), at 18–19.

[23] Hughes, 'A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (CTH)', 5 *U NSW LJ* (2001) 1, also available at: www.austlii.edu.au/au/journals/UNSWLawJl/2001/5.html.

[24] Gunasekara, 'The "Final" Privacy Frontier? Regulating Trans-Border Data Flows', 17 *Int'l J L and Info Tech* (2007) 2, at 170–176.

[25] European Commission, Data Protection Working Party, WP 9, *supra* note 14, at 2.

contractual approach to protect personal data involved in cross-border data transfer, the Consultative Committee of the Convention considered drafting relevant international model contracts to protect personal data and to regulate cross-border data transfer.[26] In fact, in several CoE recommendations on data protection the contractual approach had been proposed to protect personal privacy.[27] The Consultative Committee observed that examination of how and to what extent to require the data receiver to comply with data protection principles through contract was critically important to safeguard lawful transborder data flow and personal privacy. In 1992, a Model Contract with explanatory note was adopted by the CoE.[28] The Office of the Privacy Commissioner for Personal Data of Hong Kong, the International Chamber of Commerce (ICC), and the Canadian Chamber of Commerce followed suit.[29]

Before drafting Directive 95/46/EC, the European Commission had already been actively involved in the discussion on using model contracts to protect personal data. National practices and the CoE's adoption of the Model Contract pushed the EU to incorporate such an approach into the Directive. According to Article 26 of the Directive, where the data controller adduces adequate safeguards with respect to individuals' right to data protection, in particular through appropriate contractual clauses, data may be transferred to a third country which does not ensure an adequate level of protection. The transferor and the transferee may formulate the contract by themselves, or choose the standard contractual clauses formulated by the European Commission. The Commission may decide that certain standard contractual clauses offer a sufficient level of protection, and Member States shall take necessary measures to comply with the Commission's decision. In other words, the contractual approach is a legitimate ground for transfer of data to a third country which does not ensure an adequate level of data protection. Because it is unfeasible for the European Commission to identify a large number of countries as having an adequate data protection level and, compared with

[26] Council of Europe, Model Contract to Ensure Equivalent Protection in the Context of Transborder Data Flows with Explanatory Report, 1992, at para. 7, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2ModelContract_1992.pdf.

[27] Council of Europe, Recommendation No. R (86) 1 on the Protection of Personal Data Used for Social Security Purposes, 1986; Recommendation No. R (87) 15 on Protection of Personal Data in the Police Sector, 1987; Recommendation No. R (89) 2 on Protection of Personal Data Used for Employment Purposes, 1989, all available at: www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international%20legal%20instruments/12Recommendations%20and%20resolutions%20of%20the%20Committee%20of%20Ministers.asp#TopOfPage.

[28] Council of Europe Model Contract, *supra* note 26.

[29] Hong Kong, Office of the Privacy Commissioner for Personal Data, *Transfer of Personal Data Outside Hong Kong: Some Common Questions, Model Contract* (1997); ICC, *Model Clause for Use in Contracts Involving Transborder Data Flows* (1998); The Canadian Chamber of Commerce, *Model Contractual Clauses for Transfer of Personal Information to a Data Processor* (2002).

other exceptional cases referred to in Article 26(1), it can better protect personal data,[30] the contractual approach is preferred by the Commission.

In 1998, the Data Protection Working Party identified conditions that the contractual approach should meet to be assessed as providing an adequate level of data protection.[31] Later, based on opinions of the Working Party, the European Commission adopted Decisions 2001/497/EC and 2002/16/EC, which respectively provide standard contractual clauses for transfer of data from data controllers established in the European Union to data controllers established in third countries,[32] and transfer to data processors established in third countries.[33] By reference to its experiences, suggestions from commercial institutions, and opinions of the Working Party, the European Commission adopted Decision 2004/915/EC, which revised Decision 2001/497/EC, providing another set of standard contractual clauses for transfer of data to data controllers established in third countries. Currently, three sets of standard contractual clauses are available for transfer of data from data controllers established in the European Union to both data controllers and processors in third countries. The European Commission is very likely to adopt another decision to unify these clauses.[34]

B *Nature and Scope of Application of Standard Contractual Clauses*

Standard contractual clauses are in nature somewhere between the *ad hoc* contracts reached by the parties and legislation. Where national data protection levels are very uneven, they can complement data protection laws, simplify the procedure, and decrease the costs of transborder data transfer. The law of contract could never replace the need to legislate for data protection; contractual techniques could nevertheless be used as a sort of palliative or complement to the legal framework for data protection and transborder data flow. As long as legal lacunae subsist, such contracts may contribute to improving the protection of personal data which are communicated from one country to another with different regulations. It has, however, also been underlined that such contracts do not provide a waterproof guarantee; questions remain as to the possibilities of controlling their implementation or enforcing their clauses.[35]

[30] EC Commission, Commission Staff Working Document on the Implementation of the Commissions on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, SEC(2006)95, 20 Jan. 2006, at 2.

[31] European Commission, Data Protection Working Party, WP 9, *supra* note 14.

[32] EC Dec. 2001/497/EC of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under Dir. 95/46/EC, OJ (2001) L 181/19, Annex, Standard Contractual Clauses for the Purpose of Article 26(2) of Directive 95/46 for the Transfer of Personal Data to Third Countries which do not Ensure an Adequate Level of Protection.

[33] EC Dec. 2002/16/EC of 27 Dec. 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Dir. 95/46/EC, OJ (2002) L 6/52, Annex, Standard Contractual Clause (Processors) for the Purpose of Article 26(2) of Directive 95/46/EC for the Transfer of Personal Data to Processors Established in Third Countries which do not Ensure an Adequate Level of Data Protection.

[34] EC Commission, *supra* note 30, at 7.

[35] Council of Europe, Model Contract, *supra* note 26, at paras 12 and 13.

Model contracts on cross-border data transfer are optional. The data transferor and the transferee can freely choose whether to take relevant clauses, and to rectify certain clauses in case of necessity.[36] Unlike the CoE's Model Contract, standard contractual clauses of the EU are incorporated into its legal framework on cross-border data transfer. Of course, the legal effect of these standard contractual clauses only requires the Member States not to object that they provide adequate level of data protection. Cross-border data transfer is still subject to approval and national regulations on data processing.[37]

Model contracts on cross-border data transfer seek to coordinate the free flow of information and protection of personal data. As its Explanatory Note observes, the CoE Model Contract aims to: '(a) provide a way of resolving the complex problems which arise following the transfer of personal data subjected to different protection regimes, (b) facilitate the free circulation of personal data in the respect of privacy, (c) allow the transfer of data in the interest of international commerce, (d) promote a climate of security and certainty of international transactions involving the transfer of personal data'.[38] Standard contractual clauses may also decrease the cost of contract conclusion, and facilitate the harmonization of national rules on data protection. For example, the ICC Model Clauses are drafted to be incorporated in contracts between data exporters and data importers, reducing costs and facilitating satisfaction of the requirements of data protection authorities. Furthermore, efforts in promoting the development of commonly accepted practices and principles make a form of contract embodying important concepts acceptable to a broad spectrum of enterprises. As the forms and practices become more widely known and accepted, they are then readily adopted by the general business community.[39] The European Commission also notes that it is desirable for data controllers to be able to perform data transfers globally under a single set of data protection rules. In the absence of global data protection standards, standard contractual clauses provide an important tool allowing for the transfer of personal data from all Member States under a common set of rules.[40]

Contracts for cross-border data transfer within and outside the EU share both commonalities and differences. Both types of contracts have to split data protection obligations between the data transferor and the transferee. However, the contract for transfer of data to third countries must do more. It must provide additional safeguards for the data subject due to the fact that the transferee in the

[36] Commission Dec. 2001/497/EC, *supra* note 32, Preface, para. 5; Decision 2002/16/EC, *supra* note 33, Preface, at para. 4.

[37] Commission Decision 2001/497/EC, *supra* note 32, Arts 1 and 2; Decision 2002/16/EC, *supra* note 33, Arts 1 and 2.

[38] Council of Europe, Model Contract, *supra* note 26, at para. 23.

[39] ICC, Model Clauses, *supra* note 29, Explanatory Notes.

[40] Commission Dec. of 27 December 2004 amending Dec. 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, 2004/915/EC, OJ (2004) L 385/74, Preface, at para. 1.

third country is not subject to an enforceable set of data protection rules providing an adequate level of protection.[41]

As for the scope of application, the Model Contract of the CoE has been designed to allow for the transfer of personal data between independent economic entities. It can serve as a basis for the establishment and development of appropriate rules, e.g., for transfers within the same group of enterprises or between a file controller and a data processing service.[42] Similarly, the ICC Model Clauses apply to transborder data flow between two parties which involves personal data. They are drafted for use in a two-party transaction. This may take place between a commercial entity and a data processing service provider in another country or between two members of the same group of companies sharing human resources or other personally identifiable information.[43] Two of the three sets of standard contractual clauses of the EU, i.e., those annexed to Decisions 2001/497/EC and 2004/915/EC, apply to the transfer of data from a data controller established in the Community to data controllers established in third countries. The standard contractual clauses annexed to Decision 2002/16/EC apply to the transfer of data from a data controller established in the Community to data processors established outside the Community.

C *Sufficient Safeguards Provided by the Standard Contractual Clauses*

The abovementioned nature, status, and scope of application of the standard contractual clauses causes the European Commission to be extremely strict on the criteria for assessing the sufficiency of safeguards provided by them. Because the third country where the data transferee is established does not provide an adequate level of data protection, the Commission adopts the same criteria as in assessing data protection in third countries. In other words, both the contents and the enforcement mechanism of the standard contractual clauses have to be examined.[44] In fact, the standard contractual clauses could be seen as contractualized versions of Directive 95/46/EC.

1 *Liability Regimes*

Compared to the data importer established in third countries, the European Commission is more capable of monitoring the fulfilment of duties by the data exporter. Therefore, the standard contractual clauses of the EU make the data transferor the key party to bear liabilities for breach of contract. The Standard Contractual Clauses annexed to Decision 2001/497/EC adopt the principle of joint and several liability. The data exporter and the data importer agree that they will be jointly and severally liable for injury to the data subject resulting from any violation of their contractual obligations.[45] Joint and several liability reduces the

[41] European Commission, Data Protection Working Party, WP 9, *supra* note 14, at 3.

[42] Council of Europe, Model Contract, *supra* note 26, at para. 24.

[43] Hong Kong, Office of the Privacy Commissioner for Personal Data, Model Contract, *supra* note 29, Preface.

[44] European Commission, Data Protection Working Party, WP 9, *supra* note 14, at 4–10.

[45] Commission Dec. 2001/497/EC, *supra* note 32, Preface, at para. 19.

practical difficulties which data subjects could experience when trying to enforce their rights under the standard contractual clauses.

In consideration of the fact that joint liability puts too great a burden on the data exporter, the Clauses annexed to Decision 2004/915/EC contains a liability regime based on due diligence, where the data exporter and the data importer would be liable *vis-à-vis* the data subjects for their respective breach of their contractual obligations. The data exporter is also liable for not using reasonable efforts to determine that the data importer is able to satisfy its legal obligations under the clauses (*culpa in eligendo*). Therefore, if the data importer breaches the contract, the data subject has to go first to the data exporter, and request him to take appropriate measures to enforce his rights. If the exporter does not take measures within the proper time limit, the data subjects can go directly to the data importer to claim their rights. The data subjects are also entitled to proceed directly against a data exporter which has failed to use reasonable efforts to determine that the data importer is able to satisfy its obligations under these clauses.[46] Such a liability regime is of particular importance, in particular in connection with the ability of the data exporter to carry out audits on the data importer's premises or to request evidence of sufficient financial resources to fulfill its responsibilities.

According to Decision 2002/16/EC, the data subject should be entitled to take action and, where appropriate, receive compensation from the data exporter, who is the data controller of the personal data transferred. Exceptionally, the data subject should also be entitled to take action against the data importer in those cases, arising out of a breach by the data importer of any of his obligations, where the data exporter has factually disappeared or has ceased to exist in law or has become insolvent.[47]

2 The Third-party Beneficiary Right

To provide appropriate redress to data subjects, the standard contractual clauses endow data subjects with third-party beneficiary rights, which enable them to enforce their rights prescribed in relevant clauses.[48] According to the Data Protection Working Party, providing a legal remedy to a data subject by way of a contract between the data transferor and the recipient is not a simple question. Much will depend on the nature of the applicable contract law, since some national laws permit the creation of third party rights, whereas others do not.[49]

For data transferred from data controllers established in the Community to data processors established in third countries, the third party beneficiary clauses is helpful for the data subjects to exercise their rights under the contract

[46] Commission Decision 2004/915/EC, *supra* note 40; Standard Contractual Clauses Set II, Clause III.

[47] Commission Decision 2002/16/EC, *supra* note 33, Standard Contractual Clauses (Processors), Clause 6.

[48] Commission Decision 2001/497/EC, *supra* note 32, Standard Contractual Clauses, Clause 3; Decision 2002/16/EC, *supra* note 33, Standard Contractual Clauses (Processors), Clause 3; Decision 2004/915/EC, *supra* note 40, Standard Contractual Clauses Set II, Clause III.

[49] European Commission, Data Protection Working Party, WP 9, *supra* note 14, at 6.

and rights prescribed in national data protection laws. Indeed, European companies use processing services located outside the Union for different reasons, either for concentrating data processing facilities or for subcontracting cheaper data processing services. Some multinational organizations, in particular in the financial sector, use processing services located in different continents in order to obtain an uninterrupted 24 hours of processing operations. Large distances and national borders separate the data controller in Europe from data processors located around the globe. Although the supervisory authorities and national courts can reach the data controller, but the physical location of data may be a real problem. In those cases, where the data exporter does not for whatever reasons restrict the data importer properly, the data subjects should additionally be able to rely on the third party beneficiary clauses to enforce their data protection rights.[50]

3 *Enforcement Safeguards*

To ensure the performance of their obligations under the contract by the data exporter and the importer, the standard contractual clauses build in comparatively sound supervisory and remedy mechanisms. Unlike the law, contracts are agreements reached by the parties based on their will. Outside supervision of the performance of a contract is more difficult as well. In particular, where personal data are transferred to third countries, supervisory authorities could continue to audit, investigate, and sanction data processing carried out by the data controller established in the Union. However, for the data importer established in third countries, supervisory authorities are not capable of exercising effective control. According to the Data Protection Working Party, liability would rest with the data transferor, who need to recover any losses in a separate legal action against the recipient. Such indirect liability may be insufficient to encourage the recipient to comply with every detail of the contract.[51]

For the three sets of standard contractual clauses the European Commission is creating a supervisory mechanism on performance of the contract mainly through national supervisory authorities. They are entitled to prohibit or suspend data flow where '(a) it is established that the law to which the data importer is subject imposes upon the requirements to derogate from the relevant data protection rules which go beyond restrictions necessary in a democratic society, where those requirements are likely to have a substantial adverse effect on the guarantees provided by the standard contractual clauses; (b) refusal of the data importer to cooperate in good faith with the data protection authorities, or to comply with their clear obligations under the contract; (c) refusal of the data exporter to take appropriate measures to enforce the contract against the data importer within the normal period of one month after the

[50] European Commission, Data Protection Working Party, Opinion 7/2001 on the Draft Commission Decision (version 31 Aug. 2001) on Standard Contractual Clauses for the transfer of Personal Data to data processors established in third countries under Article 26(4) of Directive 95/46, WP 47: DG MARKT 5061/01, 13 Sept. 2001, at 4.

[51] European Commission, Data Protection Working Party, WP 9, *supra* note 14, at 10.

notice by the competent data protection authority to the data exporter'.[52] The first case seeks to avoid the impact of domestic laws on the performance of obligations by the data importer; the second is applicable where evidence of breach of contract exists; while the third resembles the anticipatory breach of contract system.

Besides external supervision, the European Commission also adds dispute settlement mechanism into the contract. In accordance with the standard contractual clauses annexed to Decisions 2001/497/EC and 2002/16/EC, where data subjects are not able to resolve disputes with the parties arising from the third party beneficiary clauses, they are entitled to: (a) bring the dispute to independent third parties, in particular the data protection authority, for mediation; (b) bring the dispute to the national courts of the data transferor; (c) bring the dispute to arbitration institutions, where the parties' home countries are parties to the 1958 New York Convention.[53]

D *Standard Contractual Clauses in Practice*

Although the European Commission is required to report on the application of standard contractual clauses, such a report was not issued until 2006.[54] For plenty of reasons, the Commission was unable to obtain adequate information. The Commission believes that the reason the Member States are unable to take note of the application of the standard contractual clauses is most likely that national supervisory authorities cannot properly monitor transborder data flow. Due to the inadequacy of information, the Commission simply concludes that problems still exist and new efforts should be made in the promotion of these clauses. In fact, the dilemma the European Commission faces is also the exact dilemma which bothers the Commission on effective monitoring of cross-border data transfer. On the surface, the European Commission builds up a firewall for personal data relating to citizens of the Union, but actual management and supervision of cross-border data transfer are difficult, or even infeasible in practice. The standard contractual clauses of the European Commission are very much like a contractualized version of Directive 95/46/EC. However, such an approach cannot encourage data transferors and data transferees to adopt the clauses and to comply with the strict data protection rules. Fortunately, the Commission has been aware of this problem, and added business clauses in consideration of the interests of corporations.

4 The Corporate Law Model and the Binding Corporate Rules

Like standard contractual clauses, the binding corporate rules (BCR) are another tool adopted by the European Commission to safeguard data protection in transborder data flow. Unlike standard contractual clauses, the BCR are not an agreement on allocation of

[52] Commission Decision 2001/497/EC, *supra* note 32, Art. 4; Decision 2002/16/EC, *supra* note 33, Art. 4; Decision 2004/915/EC, *supra* note 40, Art. 1(2).

[53] Commission Decision 2001/497/EC, *supra* note 32, Standard Contractual Clauses, Cl. 7; Decision 2002/16/EC, *supra* note 33, Standard Contractual Clauses (Processors), Cl. 7.

[54] EC Commission, *supra* note 30.

data protection obligations between the data exporter and the importer. Indeed, they are the internal operation rules of multinational corporations. If certain conditions are met, the BCR can be used to safeguard data protection in transborder data flow. The nature, objective, contents, and enforcement mechanism of the BCR are covered in a series of suggestions and recommendations issued by the Data Protection Working Party.[55]

A *BCR and Data Protection in Transborder Data Flow*

Some multinational corporations are not complicated in structure, but have affiliated organizations around the globe. Data transfers between internal companies are indispensable for the efficient operation of the group. Unlike between two independent companies, internal data transfers take place between two companies within a group, and it is not appropriate for them to conclude agreements on data transfer. The BCR are established by the Working Party as a legal ground referred to in Article 26(2) of the Directive for the transfer of data to third countries which do not ensure the adequate protection of personal data. Such kinds of rules are called Binding Corporate Rules for International Data Transfers or Legally Enforceable Corporate Rules for International Data Transfers. They are legally binding or enforceable, because only when the rules are of such a nature can they be deemed to provide the sufficient safeguards referred to in Article 26(2). The rules are corporate, because they are internal rules of multinational corporations, normally formulated by the headquarters. International data transfers are what the rules regulate.[56] In short, the BCR can be defined as legally enforceable corporate rules formulated by multinational corporations to regulate the cross-border transfer of personal data within the group.

The formulation of the BCR is a unilateral act of multinational corporations. Unlike data transfer contracts, it does not directly create rights and obligations for the parties. As for the scope of application, the BCR are mainly applied to internal data transfers between members of a group corporation. In addition, the BCR are different from codes of conduct, which are applicable to a certain type of data processing in particular sectors. Therefore, the BCR are not law. They cannot replace data protection law, and they have to operate and function within the legal framework of data protection. As for their function, the BCR are another legal ground for the transfer of data to third countries without an adequate data protection level.

B *Effectiveness of BCR*

Data protection policies of multinational corporation are generally formulated according their respective legal and cultural background, and business visions and preferences. However, to provide sufficient safeguards, the BCR have to fulfil one prerequisite, i.e., they must be internally and externally binding. Internally,

[55] European Commission, Data Protection Working Party, WP 74, 3 June 2003; WP 107, 14 Apr. 2005; WP 108, 14 Apr. 2005; WP 133, 10 Jan. 2007, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm.

[56] European Commission, Data Protection Working Party, WP 74, *supra* note 55, at 8.

companies and employees of the group have to comply with the BCR; externally, the BCR are legally enforceable by the data subjects, who can claim third party beneficiary rights. As the Working Party notes, the binding force of the BCR includes both their legal enforceability and real compliance in practice. Since the data subjects face more obstacles to the exercise of their rights in the context of cross-border data flow, the legal enforceability and real compliance of the BCR shall be ensured.[57]

C *Contents of BCR*

As for the contents of the BCR, rules on data protection, rights of the data subjects, data protection obligations of the corporation, liability, and dispute settlement are to be clarified by reference to the rules defined by the Working Party. Meanwhile, in consideration of the fact that the third country does not have a Data Protection Act or data protection tradition, the corporation shall transform abstract legal principles into directly applicable rules according to the specifics of the data transfer or the purpose of data processing. In addition, the corporation can amend the rules in accordance with changes of environment, and report the amendment to national data protection authorities.

D *Supervision on the Enforcement of BCR*

Publication of a data protection policy by the headquarters of a multinational corporation is the very first step in providing the sufficient safeguards referred to in Article 26(2) of the Directive. Meanwhile, the BCR have to establish a mechanism to ensure effective compliance with the rules both within and outside the European Union. Therefore, the corporation must make sure that the employees and members know and understand the rules by means of training programmes. Competent employees are to be appointed to monitor the application of the BCR. Secondly, the corporation must audit compliance with the BCR either by itself or through sealed auditing institutions, and report to national data protection authorities. Thirdly, in the BCR a personal complaint resolution system must be created properly and promptly to resolve disputes and complaints brought by individuals. The corporation may adopt alternative dispute resolution approaches, and request the data protection authority to become involved where necessary. Finally, the data subject shall be entitled to sue the corporation in the courts of the Member States.

The BCR approved by the European Commission look concise, but they are actually comprehensive and strict in their content. In fact, they are a corporate law version of Directive 95/46/EC. For large multinational corporations, the BCR are beneficial, eliminating obstacles to data transfers between their members companies located around the globe. However, when it comes to small- and medium-sized corporations, the strict requirement of the European Commission may scare them away. After all, without effective supervision of cross-border data transfer, they have a most inexpensive choice, i.e., to continue their data transfer, without taking any care of the strict rules or other options of the European Commission.

[57] European Commission, Data Protection Working Party, WP 12, *supra* note 11, at 5.

5 The Global Model and International Uniform Legislation

With information and communication technologies spreading across every corner of the world, data protection becomes a global concept. To safeguard the basic rights of human beings in the future, data protection has to fulfil its global mission.[58] In a way, the global model, i.e., creating legally binding international rules on data protection, is an optimal approach to resolve conflicts between the free flow of personal data and data protection. It is also the ultimate objective for data protection legislation. However, even today, great variations, differences, and conflicts still exist between national sovereignties on the nature, tradition, approach, and mechanism of data protection. Even worse, the international community lacks an appropriate and competent organization to put the vision of international uniform legislation on the agenda, and to facilitate the major information states to coordinate and adopt an international convention. The WTO seems to be capable of undertaking such a great mission, but its aims in safeguarding free international trade and its emphasis on the protection of private economic sectors make it difficult and even impossible for the WTO to fulfil such a task.[59]

It is reasonable to say that national sovereignties and domestic legislation will continue to dominate the development of data protection law, since data protection concerns the political and economic interests of each state. For a possible international convention in the future, the coordinated development of national data protection legislations is not just an obstacle. In fact, unless the majority of states have built up their respective data protection systems which best fit their national conditions, could free flow of personal data could not be possible.

Meanwhile, bilateral, regional, and multilateral collaborations between states on cross-border data protection should not be neglected.[60] Regional organizations, the European Union in particular, will continue to guide the regional unification of rules on data protection and transborder data flow. International organizations in particular fields will play a greater role in formulating international standards on data protection in certain sectors or on particular types of data. For instance, the International Civil Aviation Organization adopted in 2005 the recommended rules on processing of data relating to air passengers in the form of a supplemental document to the International Civil Aviation Convention.[61]

[58] Burkert, 'Globalization – Strategies for Data Protection', 2005, available at: www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=4231.

[59] Blume, 'Transborder Data Flow: Is There a Solution in Sight?', 8 *Int'l J L and Info Tech* (2000) 65, at 85.

[60] OECD, *supra* note 1.

[61] Abeyrantne, 'The Use of Information Contained in the Airline Passenger Name Record – Some Issues', 10 *Communications L* (2005) 55, at 170.