1
Introduction

1.1 Background

In 1999, a major US bank implemented an IT system in the US, in which it centralized its processing of employee and customer data (including data of consumers) of all its establishments around the world. The group companies obtained access on a remote basis to the data in the central IT system. This access was not limited to a group company's own employee and customer data, but also to certain data from other group companies for purposes of management information. As the US bank had establishments in most European Union *(EU)* Member States, the transfer of the employee and customer data of these EU establishments to the US and other non-EU countries triggered the EU data protection laws of these Member States. The law firm in London I worked for at the time was tasked with ensuring that these data transfers were in compliance with the EU data transfer rules. At that time this required coordination of (i) entering into the EU Standard Contractual Clauses between each of the EU data exporters (ie the EU group companies) and each of the non-EU data importers (ie the US group company that centrally processed the data as well as all other group companies established in non-EU countries that were not considered by the European Commission as providing an adequate level of data protection), and (ii) meeting all formal permit and notification requirements in these Member States. After four years we had to conclude that despite our efforts, at major cost to the client, we had not succeeded in our mission to meet all formalities in the Member States. In certain Member States, the data protection authorities, in spite of many reminders, never issued the required permits, and some never replied at all. Even worse, after four years, we had to establish that the central data processing operation had substantially changed over time, additional data categories had been added, additional central applications had been implemented (such as online performance evaluation), security measures had changed, and more. As a result, the myriad of EU Standard Contractual Clauses entered into between all group companies had become outdated, and a repeat exercise was indicated. I remember telling the client at the time, as well as my own thoughts that if I were the client, I would not repeat the exercise. Despite major efforts and costs, the compliance effort had not resulted in the desired formal compliance. But more importantly, the exercise had not brought any material data protection in practice to the employees and customers. The exercise had been performed by a network of external counsel, completely without the involvement of

the company itself. If anything, it just constituted paper compliance, shuffling contracts and permits, put in a drawer never to be looked at again. Though the contracts contained broad third-party beneficiary rights and remedies of employees and customers, the chances that these third parties would be aware of these rights and remedies were minimal (there being no requirement to publish such contracts), and if aware, the chances that employees or customers would act on these rights against the company in a foreign jurisdiction were even less.

In the same years, we regularly received instructions of multinationals, especially from outside the EU, to review their global privacy policies for compliance with EU data protection laws. These policies contained processing instructions to employees on how to process personal data of employees and customers in the performance of their tasks, and also provided for a complaints procedure if things went amiss. These reviews led to many changes in these policies, especially regarding the purposes allowed for data processing, requirements for consent and data retention, etc. These reviews did lead to actual changes in the data processing practices of the relevant multinational, and this on a global basis. Further, enquiries taught us that introduction of the internal complaints procedures led to an increase in complaints, which I took as a positive sign rather than negative, it being likely that prior to introduction of these codes, complaints were not being pursued at all rather than their not being there. My conclusion at the time was that introduction of these global privacy policies brought substantial additional material data protection to employees and customers in practice, while the administrative burden on the companies to comply with formal requirements was minimal. Money spent on external counsel was a fraction, as this concerned marking up companies' data protection policies rather than coordinating the entering into a network of formal contracts and notification and permit procedures.

Combining the two experiences led to the thought that implementation of a global privacy policy would actually prove a better tool to regulate the intercompany data transfers of multinationals than would ever be achieved by the entering into a contractual network of EU Standard Contractual Clauses. I floated the idea at some international conferences, and finally in a more public manner in the *Financieele Dagblad* of 3 April 2003:

> **Boundless Privacy**
> The Dutch Data Protection Act requires that for any exchange of personal data between group companies outside the EU, contracts need to be in place between all the group companies concerned. With a company that is even slightly multinational, this can quickly lead to hundreds of contracts. Madness.
>
> A few examples. A company implements a human resources system which contains the data of employees worldwide and which is accessible to the management of all group companies. A car manufacturer with offices over the entire world exchanges customer data with its subsidiaries in order to coordinate which clients will receive Wimbledon tickets.
>
> They should be able to do that, or so you think. All regular acts performed in the normal course of business should be acceptable and permissible. Who thinks that is thinking outside the Personal Data Protection Act. Transferring personal data, such as

employee data and data of customers of the car manufacturer, is prohibited to those countries outside the European Economic Area (EEA) that do not offer an adequate level of protection of personal data. Transferring personal data to an own group company in these countries also falls under this prohibition.

Should you forget to notify this transfer to the Dutch Data Protection Authority, then you yourself – without the approval of the customer – hang a criminal law sanction above your head. Intentional violation – you are now warned! – can lead to your doing time for six months.

Thankfully there are a few exceptions to the prohibition on transfers. But not to the duty to notify the Authority. Data transfers to group companies via a central HR system is in certain instances permissible, the most important of which are if (1) the employees concerned have provided their informed consent for the transfer, or (2) the Minister of Justice has granted a permit. Consent may be refused, and via this route it is practically not viable to transfer the complete employee processing to the group company operating the central database.

If the centralisation of the database is for management information purposes, this is only worthwhile when indeed all employee data are included. The most practical solution is to request a permit. The permit can be granted when 'adequate safeguards' to protect personal data are offered. What are adequate safeguards?

The European Commission has drafted model contracts. When the exporter of the data has concluded such model contract with the importer of the data outside the EEA, the company will receive a permit on this basis. That sounds reasonable. But how does this work out in the example of the worldwide accessible HR database? The Dutch group company then exchanges data with all its establishments outside the EEA, the French company with all establishments outside the EEA, and so on. This leads to hundreds of intercompany contracts.

It is a good thing that personal data are not, just like that, transferred to countries where there is no control over the further processing of the data. But influencing such further processing is certainly possible within a group of companies. Instead of concluding hundreds of contracts between group companies, an internal code of conduct, which all group companies adhere to, imposing strict rules for the processing of personal data, would lead to the same result. This code of conduct could provide, among other things, that the individual employees and customers involved will obtain the legal rights and remedies against the foreign group companies that they would have under their own national law.

Many companies have already implemented this type of worldwide code of conduct. Not because this was legally required, but because in a global company, all concerned have an interest in streamlining the internal procedures for data exchange. Pushing back frontiers. And now to await a model code of conduct from the European Commission.

The day after this publication, the Dutch Data Protection Commissioner (at the time Peter Hustinx), invited my (by that time Dutch) law firm and five of our multinational clients[1] to a meeting to discuss the possibility of a corporate privacy code as an alternative to the EU Standard Contractual Clauses. A working group

[1] The initial working group consisted of Philips, Shell, AkzoNobel, Sara Lee, and Heineken, at a later stage other multinationals joined such as Schlumberger, DSM, and AEGON.

was established which met regularly for the next year. In June of that year the advisory committee to the European Commission on data protection (*Working Party 29*)[2] issued the first (of a series of six) opinions on corporate privacy codes as an alternative tool for data transfers, which corporate codes it labelled 'Binding Corporate Rules' (*BCR*). Though the first opinion discussed the possibility of BCR in very general terms only, the fact that the Working Party 29 also thought the concept possible was helpful in moving the discussions in the BCR working group forward. In June 2004, the meetings and discussions resulted in a template form of BCR for employee data, which could be subsequently adapted by multinationals to their specific requirements. The discussions were based on the understanding between the Dutch data protection authority (*Dutch DPA*) and the multinationals that, while the working group was in the process of discussing how to translate the data protection requirements under the Data Protection Directive into a practical data protection compliance programme to be embodied in BCR, the Dutch DPA would not pursue these multinationals based on non-compliance in respect of their intercompany data transfers. This enabled the multinationals to spend their time and efforts on developing the compliance tools required for a data protection compliance programme, such as development of an audit programme, training modules for employees and the privacy officers, and privacy impact assessment tools. The experiences of the multinationals when developing these compliance tools, the feedback they received on the draft template BCR from their group companies around the world and review of the draft BCR by external US and other non-EU counsel, led in their turn to changes in the template BCR. Experiences were also shared with DPAs of other Member States receptive to the concept of BCR, most notably in the so-called Berlin meeting,[3] where the DPAs of a limited number of Member States and a representative of the European Commission, together with three multinationals (and their outside counsel) shared experiences in a closed meeting. The results of these discussions were fed back to the Working Party 29 and led, in turn, to the Working Party 29's five subsequent opinions on BCR. The crystallization of the BCR regime further led to the introduction of the

[2] The Working Party 29 was established as an advisory body to the European Commission under Art 29 Data Protection Directive. The Working Party 29 has advisory status only and acts independently, see Art 29(2) Data Protection Directive. Members are representatives of each of the data protection authorities (*DPAs*), the European Data Protection Supervisor and the European Commission. The tasks of the Working Party 29 are clearly formulated and are publicly available. It issues opinions to 'contribute to the uniform application of the Data Protection Directive and advises on proposals for EU legislation having an impact of data protection'. See the Document ' "Tasks of the Article 29 Data Protection Working Party', as published at <http://www.ec.europa.eu>. Though the opinions of the Working Party 29 are non-binding, they are often followed in practice by the DPAs and, as such, often set the rules de facto for application of the Data Protection Directive. The DPAs are, however, not obliged to do so and on specific topics (in particular on BCR) some DPAs follow their own course. See in more detail Chapter 6, paragraph 6.5, in particular n 51. For more detail on the Working Party 29, its tasks and procedural rules see Chapter 10, para 10.7.2–10.7.4.

[3] The meeting took place on 27 and 28 May 2004. Participants were representatives of the DPAs of Austria, Germany, Hungary, Poland, the UK, and the Netherlands, the European Commission and further GE, Philips, and DaimlerChrysler, (the multinationals at that time being most advanced in their BCR project).

mutual recognition procedure, whereby a number of DPAs agreed to mutually recognize each other's BCR authorizations.

As such, the joint development of the BCR template by the Dutch DPA and the working group of multinationals showed similarities with what my research later demonstrated to be 'learning-based meta-regulation', where legislators that aim to regulate self-regulation do so in cooperation with the companies that wish (or have to) introduce the self-regulation, based on a number of learning cycles.

My research made me realize that the development of the BCR regime constitutes a remarkable example of the emergence of a form of transnational meta-regulation (ie 'regulation of self-regulation'), whereby transnational effect is achieved not so much by transnational public regulation and transnational approvals, but by mutual recognition among national regulators of their respective publicly recognized private codes.

Another topic which attracted my attention in that period was the scope of the applicability regime of the Data Protection Directive. When advising on cross-border data processing operations, the first question to be answered is whether, and if so which of, the data protection laws of the Member States are applicable. Two trends became visible in the opinions of the Working Party 29 on the applicability regime of the Directive. Both were from a practical perspective understandable and even desirable, but were incompatible with each other and both contrary to the (legislative history of the) Data Protection Directive.

The applicability regime of the Data Protection Directive is based on the principle of cumulation of applicable laws. In the highly visible SWIFT case, SWIFT was headquartered in Belgium and had a number of establishments in the EU. Based on the cumulation principle, the central data processing operations of SWIFT in principle attract the laws of all Member States where SWIFT has an establishment. As this apparently (also in the eyes of the Working Party 29) was not desirable, the Working Party 29 applied only the law of SWIFT's headquarters (ie Belgian law) to all data processing operations of SWIFT in the EU.

On the other hand, with the increased access of EU citizens to the internet, there was an increasing number of foreign-based websites that processed data of EU citizens by means of cookies. As these foreign websites often have no establishments in the EU and do not otherwise use equipment in the EU, the protection of the Data Protection Directive does not, in principle, extend to the processing of EU data via these websites. The Working Party 29, however, qualified the computers of the users on which the cookies were placed as the 'use of equipment' in the EU and thus applied EU data protection law.

These opinions led in practice to companies filing notifications and requesting permits for data transfers which were returned by DPAs since, in their opinion, the law of their respective Member State did not apply, or conversely to a lack of compliance with EU data protection requirements as companies operating foreign websites never even thought of the possibility that the Data Protection Directive could be applicable. This widespread confusion was the trigger for my research into the applicability regime of the Data Protection Directive, which led to a number of publications and papers with recommendations for changes to the applicability

regime.[4/5] In December 2009, the Working Party 29 subsequently acknowledged for the first time that the scope of applicability of the Directive was indeed confusing, and announced it would issue a further opinion on the topic.[6] Shortly thereafter, the European Commission issued its Communication on the revision of the Data Protection Directive and announced it would indeed revise the applicability regime thereof. In December 2010, the Working Party 29 issued its further opinion on the applicability regime[7], which deviates in many instances from its earlier opinions and recommends amending the applicability regime very much along the lines as suggested in my publications.[8] At the time this book went to print the status on the thinking of the European Commission on the applicability and jurisdiction regime of the Data Protection Directive is reflected in the proposal on a new EU regulation on data protection[9] which was communicated by the European Commission on 25 January 2012[10] (*Proposed Regulation*). By choosing the form of an EU regulation as a legislative instrument instead of an EU directive, the issue of cumulation of applicable laws within the EU is to a large extent[11] solved as there will only be one data protection law that is applicable in all Member States. As to applicability of the Proposed Regulation to data processing by, for instance, foreign-based websites, the Proposed Regulation covers this as it applies to data

[4] Lokke Moerel, 'The long arm reach of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' [2011] 1 *International Data Privacy Law*, at 28–46. This publication at its turn was based on a paper presented at the 2009 ESIL-ASIL Research Forum 'Changing Futures? Science and International Law', held in Helsinki, Finland, October 2009.

[5] Lokke Moerel, 'Back to basics: when does EU data protection law apply?' [2011] 2 *International Data Privacy Law*, at 92–110. This publication in its turn draws on two earlier publications in Dutch on the interpretation by the Dutch DPA of Art 4 of the Dutch Data Protection Act, 'Back to Basics: wanneer is de Wet bescherming Persoonsgegevens van toepassing?' (2008/3) *Computerrecht*, at 81 and '"Art. 4 Wbp revisited"; naschrift De nieuwe WP Opinie inzake Search Engines' (2008/6) *Computerrecht*, at 290.

[6] See WP 168, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, as adopted on 1 December 2009 (*WP Contribution on The Future of Privacy*), at paras 26–8.

[7] Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010, 0836/10/EN WP (*WP Opinion on applicable law*).

[8] My publications in n 4 and n 5 have formed the basis for Chapters 2 and 3 of my dissertation *Binding Corporate Rules—Fixing the Regulatory Patchwork of Data Protection* (Amsterdam 2011), which I publicly defended on 19 September 2011 at Tilburg University. These chapters include the opinion of the Working Party 29 as set out in the WP Opinion on applicable law, n 7, on the respective issues.

[9] European Commission, 'Proposal for a Regulation 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' (*General Data Protection Regulation*), COM(2012) 11 final, to be found at <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>.

[10] European Commission, Communication of the Commission to the European Council, the European Economical and Social Committee of the Regions, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century, COM(2012) 9 final (25 January 2012).

[11] The Proposed Regulation leaves the regulation of certain topics to the Member States. Examples are the regulation of exemptions for data processing purposes of journalistic, artistic, or literary expression (Art 80); the regulation of data processing for health purposes (Art 81) and in the context of employment (Art 82). As a result the laws of the Member States will still deviate in certain respects. Further, the applicability regime as included in the Proposed Regulation will still lead to cumulation of these applicable national laws.

processing related to the offering of goods and services to data subjects in the EU as well as to the monitoring of their behaviour.[12]

Though much has been achieved on the topics of BCR and the applicability regime of the Directive since 2003, this is not the end of it, though. If anything it became clear in my research into the applicability regime, that the EU (like all legislators in the area of data protection) tries to use the scope of its laws to keep a grip on data when transferred across borders. By applying its law also when data are transferred abroad, the data remain protected. It also became clear to me that this is an attempt which is doomed to fail from the start. Territoriality is, and will remain, a key factor for applicable law, jurisdiction and enforcement regimes. Applicability, jurisdiction, and enforcement regimes are therefore inherently delineated and cannot be instrumental in filling the gaps in the protection of personal data and subsequent enforcement. This automatically also applies to the data transfer regimes in these laws, as these are only triggered if the relevant data protection law is applicable in the first place.

This would not pose a problem if all countries in the world were to have adequate data protection laws and enforcement. Cross-border cooperation would then be a solution to achieving protection of EU originated data. The current data protection landscape is, however, still a far cry from a proper global network of data protection laws and a global data protection standard is generally not considered achievable in the coming 10 years. This is not meant to say that we then just have to accept that control is inevitably lost over data after they have been transferred or made part of the cloud. To the contrary, it is meant to say that we have to be more creative in trying to achieve the desired cross-border protection.

When discussing and negotiating the template BCR in the BCR working group with the Dutch DPA, it became clear to me that a possible alternative for the cross-border enforcement issues inherent to the patchwork of national legislation is a choice of law and forum in BCR. Such choice of law and forum may drastically improve the data protection and the access to remedies for the individuals covered by the BCR. If a breach occurs, rather than pursuing rights through traditional judicial means, the individual affected will be able to file a complaint with the group company with which s/he has a relationship, regardless of where the breach occurred or which of the group companies was responsible for the breach. The individual will, therefore, not have to prove which of the group companies was at fault, which is one of the obstacles in practice to bringing and succeeding in a claim. There is also no issue as to which law applies and whether the relevant law provides for data protection since the breach is governed by the BCR. The complaint may be filed by the individual in her/his own language. The group company that received the complaint will be responsible for ensuring that the complaint is processed through the complaints procedure of the multinational and will ensure provision of the required translations. If the complaints procedure does not lead to a satisfying result for the individual, the group company will facilitate the filing of the complaint with the DPA

[12] Article 3(2) Proposed Regulation.

or the courts of the DPA of the chosen forum. This procedure will lead to enforceable rights even in jurisdictions where no (adequate) data protection laws are in place or where insufficient enforcement (infrastructure) is available. It further overcomes language issues and time zones and minimizes cost.

During the discussions in the BCR working group on a template form of BCR, many questions came up which were jointly solved and led to changes in the template BCR, including how to ensure that unilateral undertakings in BCR can be enforced by the beneficiaries of BCR (ie the employees and customers of the multinational). However, other questions also came up which were not easily solved and obviously required further research. One of them is whether indeed a choice of law and forum in BCR is possible or whether this contravenes the mandatory applicability and jurisdiction regime of the Data Protection Directive and/or the employee and consumer protection regimes under European rules of private international law. Further, since multinationals are not necessarily limited to the EU, recognition of BCR in the EU is not sufficient. For BCR to operate on a global basis, recognition of BCR is required also in non-EU countries for outbound data transfers from their respective countries. This requires further research whether, and if so, under which conditions, a private law instrument like BCR may be acceptable also by such non-EU countries. This is in the belief that in the present age of 'big data', cross-border solutions will not be achieved by national legislation while it is in the interest of governments, multinationals, and individuals alike to protect personal data ubiquitously.

1.2 Subject Matter and Aim of this Book

The digital era is characterized by an unprecedented continuous worldwide flow of data both within multinational companies as well as with their external service providers. While large corporations operate internationally, state governments legislate nationally. Besides leaving gaps in the patchwork of national data protection regulations, this situation also leads to overlaps in applicable national rules that often deviate or outright conflict. These conflicts make it impossible for multinational corporations to comply fully and consistently as to their many forms of cross-border data processing. Further, the traditional territory-based enforcement tools are not adequate for states to force compliance. This legal landscape provides a challenging background to test whether transnational private regulation[13] of data protection can provide solutions where legislation fails to.

[13] The term 'private regulation' is used here in the broad sense, covering both pure self-regulation and regulated self-regulation. Pure self-regulation refers to regulation processes where the state has no involvement. To describe self-regulation when it is combined with laws enacted by the state, various terms are used, such as regulated self-regulation, co-regulation, enforced self-regulation, and audited self-regulation. For a discussion on these various types, see Wolfgang Schulz and Thorsten Held, *Regulated self-regulation as a form of modern government. An analysis of case studies from media and telecommunications law* (University of Luton Press 2004), at 7.

1.2.1 Background

In the digital age, data protection is of increasing concern for governments, individuals and companies alike. While many multinational companies fully act on a seamless worldwide basis, states remain bound to their respective territories. The maturing of the internet especially led to a vast increase in cross-border flows of personal data both within and between groups of companies. Though all countries face essentially the same dilemma of how to regulate these vast flows of personal information, their governments have chosen substantially different solutions to do so. Within the EU the protection of individuals prevailed and the rights of individuals in respect of the processing of their personal data became a fundamental right and freedom. The desire to avoid gaps in the protection of personal data and to prevent circumvention of the Data Protection Directive led EU legislators to provide for a very broad scope of applicability of the Data Protection Directive ('long arm reach'). The wish to regulate the outbound transnational data streams from the EU resulted in another 'long arm' provision in the Data Protection Directive, where it prohibited data transfers to countries outside the EU without an adequate level of protection (*EU data transfer rules*). This extraterritorial provision prompted many countries outside the EU to follow suit in adopting comprehensive data protection legislation to facilitate ongoing access by their multinationals to the EU market. These states also struggled to regulate their outbound transnational data streams which resulted in many states adopting equally 'long arm reach' data protection laws and multiple instances of 'overregulation' (ie where rules are made so generally applicable that they apply prima facie to processing of personal data of their nationals wherever processed around the world). In addition, many of these countries have imposed restrictions on the outbound transfer of personal data from their respective countries. Such outbound data transfer requirements are considered necessary by most countries as there are still many countries with no data protection laws at all as well as countries (most notably the US) with a limited regime, where public regulation is targeted at certain sensitive industries and data categories only. As a consequence the worldwide data protection regulatory landscape at present consists of at best a patchwork of very diverse national data protection laws, which laws often deviate or even outright conflict.

A specific challenge for data protection regulators across the world is posed by the fact that enforcement of data protection legislation is based on a jurisdictional approach. In the international environment this leads to many long arm reach data protection laws having no hope of enforcement in practice if the relevant company is also not established in the relevant jurisdiction. Further, the concepts of applicable law and jurisdiction are embedded in a long tradition of private international law, where laws that over-extend their jurisdictional reach are considered an unacceptable form of 'hyper-regulation' if they apply so indiscriminately that there is no hope of enforcement. Applicability regimes are therefore inherently delineated and cannot be instrumental in solving the present gaps in the protection of personal data and the enforcement thereof.

At present the data protection regulators aim to solve the cross-border enforcement issues by a 'network approach', where data protection authorities of different jurisdictions cooperate in the event of cross-border violations. Until the time all jurisdictions have adequate data protection laws and supervision thereof, this network approach cannot adequately solve the enforcement issues presently faced by data protection regulators. Though there is a persistent call for a legally binding global standard for data protection and there are some concrete initiatives in this respect, it is not expected, however, that a global standard will indeed be realized within the coming 10 years. The present regulatory landscape is still too diverse for such a standard to be acceptable for adoption on a global level. In any event the adoption of a global standard should not be taken as the holy grail for all international jurisdiction and enforcement issues as presently seen in the data protection field. Even if global standards exist, differences in enforcement between countries will remain as in practice regulatory enforcement at the national level proves patchy, whether this is due to lack of resources or the prioritization by national governments of national commercial or other interests above regulatory enforcement. Solutions may therefore only be forthcoming if some form of central enforcement could be implemented by, for instance, the DPA and courts of the jurisdiction where the multinational company has its headquarters.

The existing overlap and conflicts in applicable data protection laws makes a 100 per cent worldwide compliance for multinational companies a practical impossibility. Compliance would require multinational companies not only to track and comply with the material data protection rules of each jurisdiction but also to track and comply with all requirements relating to data transfers between specific countries. Further, multinational companies largely ignore the EU data transfer rules as these lead to impossible administrative burdens. Rather than strive for compliance with the national laws on a country-by-country basis, many multinational companies implement worldwide self-regulation (by introducing corporate privacy policies). These company-wide data protection rules provide for an adequate level of data protection, and ignore possible stricter national provisions. The foregoing significantly affects the capacity of EU DPAs to enforce compliance by multinational companies in the area of data protection. The introduction of corporate privacy policies by multinational companies has created a bottom-up pressure on national legal orders. This is reflected in how third-party beneficiaries of such policies invoke them before national courts (so far mainly in the US), and the pressure exerted on the EU DPAs to recognize these corporate privacy policies as instruments to ensure an adequate level of data protection throughout the group of companies, justifying the international transfers of data between the individual group companies, wherever located. The Working Party 29[14] recognizes the added value of transnational private regulation (*TPR*) in the data protection area in light of the gaps and deficiencies of the present EU data transfer regime. The Working Party 29 set criteria for this TPR to provide for a minimum level of protection for

[14] See on the Working Party 29 n 2.

the processing of data by a multinational on a worldwide basis. With BCR, the Working Party 29 introduced a complex hybrid system of self-regulation (corporate privacy policies) with public arrangements (the DPAs validating such corporate privacy policies and providing support in the area of enforcement). The BCR regime established by the Working Party 29 introduces the possibility of worldwide central enforcement of such BCR by the DPA and courts of the EU headquarters of the multinationals.

The regulatory environment described above, and the deficiencies in protection and enforcement make a challenging background to research whether any gaps and deficiencies in the present applicability and jurisdiction regime of the Data Protection Directive may be addressed by transnational self-regulation, rather than by long arm jurisdiction-based legislation and jurisdiction-based enforcement. Of special interest in that context are the relative merits of central enforcement of BCR through one lead DPA (this lead DPA taking over the enforcement from other DPAs in their respective territories) over the present reliance on enforcement on a network basis (whereby DPAs cooperate in the enforcement in order to enable each DPA to enforce on its own territory).

1.2.2 Aim of this book

Assessment of the suitability and relative merits of corporate self-regulation of data protection as an instrument to regulate global data transfers

In the recent past a vast body of research has been conducted into:

(i) the legitimacy of TPR to regulate corporate conduct in a globalized society;

(ii) how TPR can be aligned with principles of private international law (*PIL*)

(iii) how TPR can be used to implement the 'principle of accountability' in respect of compliance with the relevant legal requirements; and

(iv) the area of corporate social responsibility (*CSR*), where multinationals also implement TPR to overcome differences in regulations and regulatory approaches between countries and as part of their global reputation management.

None of the research above addresses specifically that of TPR regulating data protection in an international environment. Also, the Working Party 29 and the DPAs have little experience with TPR as a tool to regulate cross-border data compliance. Though the Working Party 29 has recently approved the concept of BCR, some DPAs still struggle with the requirements under which these BCR can be recognized and enforced. Similar uncertainty exists as how to fit the BCR concept with the regulatory data protection regimes of other countries or regions like the APEC Privacy Framework. Given this lack of experience, I assess the BCR regime in light of the findings of existing general research into the legal arenas above. Two main topics I address are to what extent data protection may be regulated by TPR and whether a choice of law and forum is allowed under PIL

so that indeed central enforcement of BCR is possible. This book results in proposals for improvement of the BCR regime as well as proposals as to how to fit this hybrid system with other existing data protection regimes across the world (especially in the US) and new regulatory regimes in development today (especially by the APEC countries). The objective is to investigate how to further the acceptance of BCR as a mainstream global solution to regulate global corporate conduct in the area of data protection. BCR may then indeed provide a private solution to solve the gaps in protection and enforcement as presented by the current patchwork of national data protection laws and jurisdiction based enforcement thereof.

Part of this assessment will also be to test the following hypotheses:

(i) BCR as an instance of TPR can do better than the present territory-based state regulation of data protection in terms of:
   (a) avoiding gaps in protection and enforcement as presented by the current patchwork of national data protection laws and state-based enforcement; and
   (b) regulating transborder data flows.

(ii) The BCR regime as currently developed by the Working Party 29 does not sufficiently incorporate or is not sufficiently aligned with principles of PIL, best practices when implementing the principle of accountability, generally accepted legitimacy demands made of TPR, and best practices as to CSR, in order for BCR to be acceptable on a global basis as a form of TPR to regulate global corporate conduct in the area of data protection (societal relevance).

1.2.3 Relevance and recommendations

With this book, I intend to (i) contribute to the academic debate on these topics; (ii) further the acceptance of BCR as a mainstream global solution to regulate global corporate conduct in the area of data protection (societal relevance); and (iii) provide concrete suggestions to EU legislators on how to improve these regimes.

Re (i) Academic relevance

The academic relevance of my research has already been addressed in the previous paragraphs. In addition, I mention that the assessment of the BCR concept in particular in light of the findings of the existing research into the legitimacy of TPR to regulate corporate conduct in a globalized society, adds an interesting concrete example in practice to test the merits of these findings. This is particularly relevant as under EU law data protection qualifies as a human right,[15] and the existing literature is divided on the issue whether human rights are indeed fit to be regulated by TPR (and in particular CSR codes) and the existing research has until now not

[15] See in detail Chapter 3, n 3.

been extended to the role of self-regulation in the data protection field.[16] The BCR regime constitutes further a remarkable example of the emergence of a form of transnational meta-regulation (ie 'regulation of self-regulation'), whereby transnational effect is achieved not so much by transnational public regulation and transnational approvals, but by mutual recognition among national regulators of their respective publicly recognized private codes.

Re (ii) Further acceptance of BCR as mainstream solution (societal relevance)

The substantial efforts and cost for multinationals to embark on a worldwide BCR programme without having certainty (i) whether the BCR concept will work on an EU wide basis; and (ii) about the time frame within which EU-wide approval of BCR may ultimately be achieved, prove an obstacle in practice for multinationals to decide on the adoption of BCR within their group of companies. Multinationals will benefit if the uncertainties as to the validity and enforcement of BCR are solved and the BCR authorization procedure is streamlined. Given the present non-compliance by multinationals with the EU data transfer rules and the cross-border enforcement issues encountered by individuals in the enforcement of their rights, individuals may equally benefit.

The assessment of the BCR regime in light of the findings of existing research on TPR, PIL, CSR, and the accountability principle will accelerate the acceptance and credibility of BCR as the mainstream global solution. This is not only beneficial to multinationals, but at the same time will also enhance the protection afforded to individuals of one of their fundamental rights and freedoms.

Re (iii) Recommendations to EU legislators

My suggestions to EU legislators for improvement are not made collectively at the end, but rather throughout the text where indicated and are placed in a framework. An overview of my recommendations can be found in Chapter 12 and further in Annex I, which also provides a matrix listing for each recommendation which of the disciplines led to such recommendation, as well as whether such recommendation overlaps with those made for revision of the Data Protection Directive by the Rand Report, the Working Party 29, the European Data Protection Supervisor, the Centre for Information Policy Leadership, and/or the European Commission.

1.2.4 Prior research and publications

This book has already been published as Part II of my dissertation *BCR—Fixing the Regulatory Patchwork of Data Protection*,[17] which I publicly defended at Tilburg University on 11 September 2011. Changes to the text have been limited to attune

[16] Several case studies in respect of TPR of human rights (including BCR) are presently performed as part of the HiiL Program (see on the HiiL Program para 1.2.4).

[17] See n 8.

the text to the fact that I have left out Part I of my dissertation on the applicability and jurisdiction regime of the Data Protection Directive. Further, I have included new text and footnotes to show the changes to EU data protection law as proposed in the Proposed Regulation.[18] Though I left out Part I of my dissertation, the current text in many aspects relies on the prior research on the applicability and jurisdiction regime of the Data Protection Directive.[19]

For this book I have further made use of my desk research[20] performed as part of the HiiL Research Program 'Private Actors and Self-Regulation', into the legitimacy, effectiveness, enforcement, and quality of different forms of TPR (*HiiL Program*).[21] As part of the HiiL Program, I carry out a case study into the legitimacy, effectiveness, enforcement, and quality of BCR as a form of TPR of data protection. The empirical research in respect of the effectiveness of BCR in providing material data protection to individuals is outside the scope of this publication, but is currently being conducted as part of the HiiL Program, and will be published at a later stage.[22]

[18] See n 9.

[19] See n 4, n 5 and further Part I of my dissertation (n 8).

[20] In particular my paper 'Transnational Private Regulation of Data Protection' prepared for the 2010 HiiL Annual Conference on Transnational Private Regulation, June 2010, Dublin, to be found at <http://www.privateregulation.eu>.

[21] For the scope of the HiiL Program's research, see HiiL 2008, 'The Added Value of Private Regulation in an International world? Towards a Model for the Legitimacy, Effectiveness, Enforcement and Quality of Private Regulation' and the 'Draft Inventory Report', both dated May 2008 and to be found at <http://www.hagueppgnetwork.org/topics-the-hppgn/>. The central research questions of the HiiL Program are set out in the Draft Inventory Report, at para 2.5:

1. Is regulation with a transnational dimension, drafted by private actors, more successful than formal, state-regulation in regulating the conduct of corporations active in the global market?
2. If so, to what extent, under what conditions and with respect to which areas does private regulation have a—positive or negative—impact upon the effective and efficient functioning of national legal orders?
3. The main objective of the research is to formulate a model (or a number of models), which could be of use to governments and to private actors, in which these questions come together and be answered.

The HiiL Program will, on a theoretical level, research the following topics:

- What are the transnational constitutional foundations of private regulation;
- What are the differences between private regulation at national and transnational level: what contrasting modes of acquiring legitimacy and effectiveness are adopted;
- What is the role of private regulation as an alternative or a complement to public regulation (are there common principles that can be identified?);
- What factors or principles are—or should be—relevant/decisive in making regulatory choices from the point of view of effectiveness (including learning), enforcement, legitimacy, and quality? (normative determinants);
- What are the unintended (and potentially counterproductive) effects associated with the emergence of a plurality of legal regimes at transnational level in terms both of effectiveness and legitimacy?
- What is the role of regulatory impact assessment concerning the choice between public and private regulation and the principle of proportionality?

[22] The final report of the HiiL Program is expected in December 2012.

1.2.5 Scope

This book does not concern itself with the desirability of data protection legislation per se or the relative merits of the different regulatory systems set up by legislators across the world. Multinationals have to operate in the present regulatory landscape and for this book this is taken as a given.

I further concentrate on the topic of cross-border data protection and enforcement in the private sector. This concerns cross-border flows of personal data both within groups of companies and between groups of companies. Though many types of cross-border data flows are carried out between public authorities and further between companies and public authorities (especially for law enforcement purposes), these types of data flows give rise to special issues and are outside the scope of this book.

The point of departure for this book is that data protection regulation should be designed and evaluated based on whether rules provide for material data protection for individuals in practice rather than whether they provide for rights and remedies in theory.[23]

This book is current up to 1 February 2012, and all hyperlinks were valid on that date.

1.3 Outline

Chapter 2 contains an introduction to the concept of Binding Corporate Rules and the topics discussed in this book.

Chapter 3 gives an introduction to the worldwide data protection regulatory landscape and the different types of regulatory systems. An overview is given of the basic principles of the Data Protection Directive (and the changes envisaged by the Proposed Regulation), as knowledge of these principles is required for a proper understanding of the BCR regime. The APEC Privacy Framework is also discussed as a representative of a data protection system based on an organizational approach rather than a territorial approach.

Chapter 4 discusses some trends and developments in the regulatory landscape, such as the increasing tensions between the different regulatory systems, the prospects of the growing call for a global data protection standard, and the cross-border enforcement issues presently encountered by DPAs and individuals alike. The chapter concludes with a discussion of possible alternative solutions to improve the position of individuals in case of cross-border data protection violations. One of

[23] In July 2010, the Working Party 29 explicitly embraced this perspective of 'law in action' as opposed to 'law in theory': see WP 173, Opinion 3/2010 on the principle of accountability adopted on 13 July 2010 (*WP Opinion on the principle of accountability*) at 3: 'Data protection must move from "theory to practice". Legal requirements must be translated into real data protection measures. (. . .) In its document on The Future of Privacy (WP 168) of December 2009, the Article 29 Working Party expressed the view that the present legal framework has not been successful in ensuring that data protection requirements translate into effective mechanisms that deliver real protection.'

these solutions requires the introduction by multinationals of global corporate self-regulation backed up by government enforcement. By introducing the possibility for multinationals to make a choice of law and forum in these self-regulatory codes, it would be possible to have these codes supervised and enforced on a worldwide basis by one 'lead' DPA (*Lead DPA*) only, preferably the authority of the place of establishment of the headquarters of such multinational.

Chapter 5 discusses a number of practical developments encountered by multinationals, which result in the data processing operations of multinationals being governed by a myriad of national data protection laws. It is subsequently discussed why and how multinationals mitigate their global data protection risks by means of a global corporate privacy code.

Chapter 6 introduces the BCR regime as developed by the Working Party 29, recognizing corporate self-regulation as an alternative method for multinationals to comply with the EU data transfer rules. The European BCR approval procedure is discussed as well as its shortcomings. It is further discussed in which non-EU countries BCR are (potentially) recognized as a valid data transfer tool also for data transfers from these non-EU countries. Recommendations are made to recognize BCR as a valid tool for data transfers when revising the Directive and to streamline the BCR authorization procedure.

Chapter 7 discusses some contractual issues in light of the requirement that BCR should be internally binding on the group companies and employees of the multinational and externally binding for the benefit of the beneficiaries of BCR. The latter requires discussion of the enforceability of unilateral undertakings by the beneficiaries of BCR. TPR is further often effectuated through contractual 'supply chain management', a solution which is also part of the BCR regime. Also supply chain management raises issues of enforceability by the beneficiaries of these contracts, which are of equal relevance to BCR. How the various supply chain issues can be best addressed in BCR is also discussed.

Chapter 8 discusses the interaction of BCR with rules of PIL, which is twofold. First there is the traditional function of PIL, where for instance a choice of law and forum made in BCR has to comply with rules of PIL. This requires answering the questions of (i) which instruments of PIL are in scope?; do the rules of PIL take precedence over the applicability and jurisdiction regime of the Directive?; and (iii) is a choice of law possible under the Directive? It is further discussed how the BCR applicability and enforcement regime can be best set up to avoid the current pitfalls under the employee and consumer protection regimes of PIL. The second function of PIL is as a potential source of 'meta-norms' for BCR. It is discussed how the BCR applicability and enforcement regime can be best aligned with the underlying policy choices behind PIL instruments and doctrines in order to be able to achieve universal acceptance of BCR.

Chapter 9 discusses BCR in the wider context of the introduction of the 'accountability principle' in the area of data protection and in other fields of law. Specific attention is devoted as to how regulators can provide companies with incentives and tools to use their own inherent 'regulatory capacities'. Separately discussed are the merits and the relevance for BCR of the proposal by the Working

Party 29 to introduce in the revised Directive a provision that controllers will remain accountable for the protection of their data even after these data have been transferred to a third party.

Chapter 10 evaluates BCR as a form of TPR. This concerns the issue of what the optimal form of meta-regulation is when choosing TPR. The discipline of how best to regulate (the rules for rule-making, the search for meta-norms) has in the EU become known under the label 'Better Regulation' (*BR*). In this chapter BCR are evaluated from the perspective of BR as to (i) whether the norm-setting as to BCR meets the basic requirements for EU law-making, for instance as to requirements of participation and transparency; and (ii) whether BCR (qualifying as co-regulation) concern an area of law for which EU legislators consider co- or self-regulation appropriate. Proposals are made to bring the BCR norm-setting, evaluation/monitoring, and enforcement in line with the body of thought on BR.

Chapter 11 addresses BCR as a form of CSR. It is discussed to what extent data protection is covered by international soft law instruments setting guidelines for CSR, and if so, whether this has any repercussions for the BCR regime. This requires (again) a discussion of regulating human rights, not so much in the context of whether these may be regulated by self-regulation, but whether the international instruments on CSR require that fundamental rights held by individuals should be viewed as imposing duties directly on multinationals, even for activities of these multinationals in countries that do not recognize such human rights.

Chapter 12 presents my overall conclusions and recommendations and gives an evaluation of the research objectives and hypotheses.