Singapore Journal of Legal Studies
[2004] 511–546

EUROPEAN UNION DATA PROTECTION DIRECTIVE: ADEQUACY OF DATA PROTECTION IN SINGAPORE

VILI **LEHDONVIRTA***

The European Union *Data Protection Directive* requires member states to place restrictions on transfers of personal data to countries that cannot guarantee an adequate level of data protection. Countries that do guarantee adequate protection enjoy a smooth business environment and an enhanced ability to participate in trade. In this paper I examine the adequacy of Singapore's data protection regime, and in particular the Model Data Protection Code. I suggest various amendments to the regime to enable Singapore to meet the *Directive* requirements. To carry out the assessment, I use a framework developed by the Article 29 Working Party, the body that in practice carries out the official adequacy assessments for the EU.

I. INTRODUCTION

Data protection is the area of law that seeks to uphold an individual's limited right to privacy by regulating the collection, use and dissemination of personal information[1] regarding the individual. Data protection is of growing relevance today, as information technology systems become involved in more and more aspects of human life. There is considerable international consensus on the principles of data protection required to implement a measure of privacy necessary in a democratic state.[2] However, implementation of data protection regimes varies across the globe, with adverse effects for both businesses and consumers.

For consumers, this fragmentation reduces privacy. Organisations operating across jurisdictions can abuse the differences between the regimes to circumvent data protection. The process of managing personal information can be split into several stages, and each stage carried out in the jurisdiction that least restricts it. The

---

* B.Sc. (Tech.) (Helsinki). I am currently pursuing an interdisciplinary M.Sc. at the Helsinki University of Technology, as part of which I had the wonderful opportunity to spend the academic year 2003–2004 at the Faculty of Law, National University of Singapore. I thank Assoc. Prof. Daniel Seng for his stimulating IT law seminars, which inspired this article. Note that data protection issues are rapidly evolving, and the materials and information I have relied on are correct as at 1 May 2004. A number of materials that are cited in this article are only available online. This is sometimes unavoidable, as those materials are often the very subject of study. If readers have difficulty accessing a document at a given address, I suggest that they check if an archived version of the document is available, online: Internet Archive <http://www.archive.org/>.

1 "'Personal data' shall mean any information relating to an identified or identifiable natural person", *Data Protection Directive*, art. 2(a), *infra* note 3. I use the terms "personal information" and "personal data" interchangeably in this article. The term "individual" is used interchangeably with "data subject", and "organisation" with "data controller".

2 Joel R. Reidenberg, "Cyberspace And Privacy: A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules in Cyberspace" (2000) 52 Stan. L. Rev. 1315 at 1327-8.

overall effect of this 'cherry picking' is reduced privacy for individuals. For businesses, the fragmentation means additional costs. It imposes several different sets of rules on multi-national corporations and partnerships, which drives up compliance costs. In addition, consumers' concerns over privacy are adversely reflected in sales.

In 1995, the European Union ('EU') passed a directive concerning data protection.[3] The purpose of this *Data Protection Directive* is to harmonise data protection law within the community, aiding the development of the European inner market while simultaneously improving consumer protection. An important feature of the *Directive* is the restrictions it places on transfers of personal information to countries outside the EU. The restrictions are necessary to ensure that the purposes of the *Directive* cannot be undermined by moving data processing operations outside of the community. Article 25(1) of the *Directive* states:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing[4] or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

Transfers to countries that do not meet the adequacy criteria are allowed only after the originating party takes additional measures to ensure that the data is adequately protected abroad. National data protection authorities in the EU Member States have the final authority to forbid or permit transfers.[5]

Trans-border flows of personal data are a ubiquitous feature of global commerce today. They are not restricted to business that is conducted electronically. All multinational companies regardless of sector have a need to communicate information stored in customer, marketing and employee databases across jurisdictions. Restrictions and regulations concerning trans-border flows of data are an aspect of the business environment of a given country. A country that can ensure a smooth flow of information attracts business.[6] Raymond Tang, the Privacy Commissioner of Hong Kong, said last year: "Hong Kong economy could not afford to be competitively disadvantaged by not having a legal data protection regime that met the requirements of the EU Directive".[7]

The same will apply to Singapore, an aspiring "international e-commerce hub." In 1998, the government launched an initiative to develop Singapore into an attractive platform for the rapidly growing international electronic commerce activities. The

---

3 EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L. 281/31 [*Data Protection Directive*].

4 "Processing" is a central concept in the *Directive*. It includes not only all forms of use, alteration and adaptation, but also all collection, recording, dissemination and disclosure: *Data Protection Directive*, art. 2(b), *ibid.* This meaning is used throughout the article.

5 *Data Protection Directive*, art. 26(2), *supra* note 3.

6 The additional contractual measures needed to transfer personal information from within the EU to a country with inadequate data protection might result in additional costs to companies involved in the transfer, but this would need to be verified with an empirical study.

7 Raymond Tang, "A Short Paper on Implementing Data Privacy Principles: How Are Governments Making it Work in the Real World?" (Paper presented to the APEC Data Privacy Workshop, Chiang Rai, Thailand, 13 February 2003), online: Office of the Privacy Commissioner for Personal Data, Hong Kong <http://www.pco.org.hk/english/infocentre/ apec_feb03.html>.

initiative seeks to position Singapore as a "trusted node", calling for harmonisation of relevant laws and policies with international practices, and identifies data protection law as one of the focus areas.[8] The EU is Singapore's third largest trading partner,[9] and others, including United States, its second largest, are adopting the EU *Directive's* data protection practices.

A report published by the National Internet Advisory Committee Legal Subcommittee in 2002 was perhaps the first paper to recognise the need for a harmonised, *Directive*-adequate data protection regime in Singapore.[10] The report began work on building such a regime by introducing a set of data protection rules that later evolved into the Model Data Protection Code ('MDPC'), which is now in use in a co-regulatory data protection scheme. However, there is still some way to go before Singapore can claim to provide an "adequate level of protection."

This article aims to establish the extent to which data protection in Singapore measures up to the requirements of the EU *Data Protection Directive* today, and what could be done to bring it into compliance. Part II describes how personal data is currently protected in Singapore by a myriad of laws and other instruments. Part III argues that the correct way to evaluate the level of protection is to follow the framework developed by the Article 29 Working Party, an expert advisory body under the European Commission. Parts IV and V assess the Singapore system in regard to scope, processes, enforcement mechanisms and substantive content, and give recommendations on how to amend it. In Part IV, I come to the preliminary conclusion that only an omnibus regime will suffice, and so in Part V, I forego the fragmented mosaic of other data protection rules and focus solely on the Model Data Protection Code.

Having to send one's privacy laws to be evaluated by the European Union might seem like an attempt on EU's part to extend its legislative jurisdiction beyond the territorial boundaries of the Member States. This is not necessarily the case, however. The stated purpose of Article 25 is to protect the privacy of EU citizens.[11] If a third country chooses to extend the same protection to its own citizens, it is a sovereign decision. Nevertheless, there are ample moral and practical reasons to do so.[12]

II. Protection of Personal Data in Singapore

Singapore presently has no omnibus privacy or data protection law. Personal data is protected to some extent by a multitude of different laws, each of limited scope and application. The need for more comprehensive data protection has now been

---

8 Infocomm Development Authority, Press Release, "Singapore Launches Electronic Commerce Masterplan" (23 September 1998), online: Infocomm Development Authority <http://www.ida.gov.sg>.

9 Ministry of Trade and Industry, *Economic Survey of Singapore 2003* (Singapore: Ministry of Trade and Industry, 2004) at 146-7.

10 National Internet Advisory Committee Legal Subcommittee, "Report On A Model Data Protection Code For The Private Sector" (February 2002) at 11-15, online: Media Dev. Authority <http://www.mda.gov.sg/MDA/documents/Report_on_a_Model_Data_Protection_Code.PDF> [*Report on a Model Data Protection Code*].

11 But the purported head of jurisdiction is not nationality, either. *Data Protection Directive*, art. 25, *supra* note 3 only protects data streams originating from the EU. Singapore remains free to legislate on personal information collected from a European national who is visiting the island state.

12 See text under heading "2. *Scope with regard to the data subject*" for some discussion on this.

recognised, and voluntary self- and co-regulation schemes are being offered as the answer. But for now, data protection in Singapore remains a "tapestry of lacunae with occasional densities of normativity."[13] I first discuss the mosaic of actual laws related to data protection, and then examine the emergence of the voluntary schemes. The leading voluntary code of conduct, the Model Data Protection Code, is then introduced.

A. *Common Law*

The prevailing view in common law is that no enforceable right to privacy has yet developed.[14] Acts amounting to a breach of privacy may nevertheless infringe on some other rights under common law. Michael Hwang and Andrew Chan[15] suggest that the laws of harassment, private nuisance, trespass, defamation and confidentiality may in some circumstances provide remedies for privacy intrusions in this indirect way. Data protection regimes typically seek to protect data privacy through the establishment of rights for the individual and obligations for the data controller. In this respect there is overlap between data protection and the torts suggested by Hwang and Chan, even if their goals are different. What follows is a brief overview of the applicability of Hwang and Chan's torts for various purposes generally associated with data protection.

Private nuisance has some merit in data protection: in the Canadian case of *Motherwell v. Motherwell*[16] and the English *Khorasandjian v. Bush*,[17] it was used to provide remedies for unwanted phone calls and, in *Motherwell*, for unwanted mail.[18] This is highly relevant, because one important issue in data protection is the individual's right to refuse direct marketing, a subset of unsolicited communications.[19] However, private nuisance is a tort against the enjoyment of land. The House of Lords reaffirmed in *Hunter v. Canary Wharf Ltd*[20] that a person must have an interest in the land to have standing to sue. The tort of trespass is also similarly linked with land.[21] Thus nuisance and trespass can provide a remedy against unwanted communications in very specific circumstances only. In this age of mobile communications, the usefulness of these torts for data protection is very limited. The recent Singapore case *Malcomson v. Naresh*[22] also dealt with unwanted communications: repeated phone calls, SMS messages and e-mail. The finding was harassment, which is not linked to

---

13 The phrase is borrowed from Carty who used it to refer to public international law in Anthony Carty, "Critical International Law: Recent Trends in the Theory of International Law" (1991) 2 E.J.I.L. 66 at 75.

14 Michael Hwang & Andrew Chan, "Singapore" in Michael Henry ed., *International Privacy, Publicity & Personality Laws* (London: Butterworths, 2001) at 356; Looi Teck Kheong, "Should there be Privacy laws in Singapore?" *Singapore Law Gazette* (February 2001) 19.

15 Michael Hwang & Andrew Chan, *ibid.*

16 (1976) 73 D.L.R. 62.

17 [1993] 3 All E.R. 669.

18 Michael Hwang & Andrew Chan, *supra* note 14 at 368-9.

19 See "*H. Direct Marketing*" below.

20 [1997] 2 All E.R. 426.

21 Michael Hwang & Andrew Chan, *supra* note 14 at 370.

22 [2001] 3 S.L.R. 454.

land like nuisance and trespass. It is a long way from *Malcomson* to a general right to forbid the use of one's personal data for direct marketing, though.

An important goal of data protection regimes is to provide individuals with some control over the use and disclosure of their personal information.[23] The laws of confidentiality and defamation could be useful to this end. The law of defamation can provide individuals with means to restrict the publication of some statements regarding them, and a remedy after the fact. A classic definition of defamation in common law is "words which tend to lower the person in the estimation of right-thinking members of society generally".[24] A more recent test that has been applied in Singapore asks whether the claimant has suffered injury in the claimant's office, profession or trade.[25] Another test, said to possess special potential for privacy protection, asks if the claimant was made the object of ridicule.[26] What all the tests have in common is that they disregard the claimant's subjective view and let "hypothetical referees" decide whether a statement is covered or not.[27] Data protection, on the other hand, generally extends to all personal information.[28] This gives individuals the power to determine, based on their own subjective views, what information they want to keep private and what information they are comfortable with publicising.[29] This is consistent with the fact that the notion of 'privacy' is subjective to each individual.

Typical pieces of personal information that a person might want to keep private for any reason include home address, phone number, salary and favourite web site. Yet their publication seems unlikely to trigger any of the above tests in normal circumstances. Some pieces of personal information such as those related with an individual's medical history can be more sensitive in nature, and they would probably pass the above tests more readily. But truth is a complete defence to defamation.[30] As far as the information is accurate, the law of defamation will generally speaking not provide a remedy against its publication.[31]

The law of confidence is currently the main instrument for policing misuses of private confidential information in British Commonwealth courts.[32] It is very topical from a data protection point of view, because in the recent English case of *Douglas and Others v. Hello! Ltd. and Others (No. 3)*[33] the claimant was awarded damages under both breach of confidence as well as the U.K. *Data Protection Act 1998*[34] (which implements the *Data Protection Directive* in the U.K.). It was partly the same

---

23 See text accompanying "A. *The Purpose Limitation* Principle" below.

24 *Sim v. Stretch* [1936] 2 All E.R. 1237 at 1240.

25 F. A. Trindade, "When is Matter Considered 'Defamatory' by the Courts?" [1999] Sing. J.L.S. 1 at 8.

26 *Ibid.* at 10.

27 *Ibid.* at 14.

28 See definition in *supra* note 1.

29 I hasten to add that the same kind of public interest and freedom of expression defences that exist in defamation are also found in data protection laws. See e.g. *Data Protection Directive*, art. 7(e), 9, *supra* note 3.

30 See e.g. *Reynolds v. Times Newspapers Ltd and Ors.* [2001] 2 A.C. 127 at 192. In the local case of *Goh Chok Tong v. Tang Liang Hong* [1997] 2 S.L.R. 641, the defendant pleaded truth (justification) but was unsuccessful in establishing it.

31 On the other hand, this introduces an incentive for organisations to keep their records accurate, which is another goal of data protection. See text accompanying "B. *The Data Quality and* Proportionality Principle" below.

32 Megan Richardson, "The Private Life After *Douglas v. Hello!*" [2003] Sing. J.L.S. 311 at 327.

33 [2003] All E.R. 996.

34 *Data Protection Act 1998* (U.K.), 1998, c. 29 [*Data Protection Act 1998*].

facts that gave rise to the liability under both common law and the *Data Protection Act*, which makes the case a definite example of overlap between the two. Megan Richardson[35] provides a discussion on the use of confidentiality for privacy protection that takes *Douglas v. Hello!* into account. She finds that the doctrine has evolved to respond to privacy issues such as the case in question, but does concede that it remains centred around the concept of publication.[36] Despite its merits in privacy protection, the law of confidence is therefore not a substitute for a data protection regime that embraces the complete life-cycle of a piece of personal data, from collection through use to any disclosure.

Douglas v. Hello! and *Dow Jones & Company, Inc v. Gutnick*[37] demonstrate how globalisation and the internet are making geographical boundaries of jurisdictions irrelevant when it comes to privacy issues. This prompts Richardson to call for harmonisation of common law.[38] But that would limit the extent of privacy harmonisation to common law jurisdictions only. I say harmonise statutes instead.

B. *Statutes*

Although no general privacy or data protection act has been passed in Singapore, there are many statutes that touch upon the processing of personal data in one context or another. Statutes that govern various public sector uses of personal data include the *Official Secrets Act*,[39] *Statistics Act*,[40] *Central Provident Fund Act*[41] and the *Electronic Transactions Act*.[42] Typically these statutes provide that information acquired through exercise of powers under the Act must not be disclosed except as required by law.[43] Similar statutes that apply to parts of the private sector include the *Banking Act*[44] and the *Telecommunications Act*.[45]

The *Computer Misuse Act* is related to electronic privacy in the way that it criminalises, *inter alia*, the accessing of information in a computer system without authority.[46] In other words, outright data theft is outlawed. However, the *Computer Misuse Act* does nothing to regulate the collection, use and disclosure of personal information acquired by *prima facie* lawful means. It is not designed for general data protection. The Act could, perhaps, be used to restrict some forms of invasive data harvesting conducted by internet businesses on their customers.

A presentation given by a director at the Infocomm Development Authority of Singapore ('IDA') boasted that Singapore has "more than 150 laws with privacy

---

35 *Supra* note 32.
36 *Supra* note 32 at 328-9.
37 [2002] HCA 56.
38 *Supra* note 32 at 332.
39 Cap. 213, 1985 Rev. Ed. Sing.
40 Cap. 317, 1999 Rev. Ed. Sing.
41 Cap. 36, 2001 Rev. Ed. Sing.
42 Cap. 88, 1999 Rev. Ed. Sing.
43 Goh Seow Hiong, "Data Protection & Privacy in Singapore" (Presentation at the Asian Personal Data Privacy Forum, Hong Kong SAR, 27 March 2001), online: Office of the Privacy Commissioner of Personal Data, Hong Kong <http://www.pco.org.hk/misc/singapor/sld001.htm>.
44 Cap. 19, 2003 Rev. Ed. Sing.
45 Cap. 323, 2000 Rev. Ed. Sing.
46 Cap. 50A, 1998 Rev. Ed. Sing., s. 3.

provisions."[47] This is perhaps a slight mischaracterisation: 161 statutes have been found to have "secrecy and disclosure provisions",[48] but such provisions constitute privacy protection only when their subject matter is personal information and not *e.g.* governmental secrets or the accounts of a corporate entity.[49] Later I examine whether a large number of privacy laws is something to be delighted about in any case.[50]

Copyright law has been suggested to provide a level of protection for personal data.[51] The theory is that since copyright grants the author a right to stop others from publicising and distributing the subject matter, it would effectively equate to data protection when the subject matter is personal data.[52] In my view this is a mismatch. The biggest problem is that typical pieces of personal data, whether they be contact details, web clickstreams or shopping preferences, hardly attract copyright protection. In cases where the data does attract copyright protection, for example with CCTV video material, the owner of the copyright might not be the data subject—the owner might be the data controller! That would turn the "copyright data protection regime" on its head.

C. *Self-regulation and Co-regulation*

As businesses and governmental bodies in Singapore are gradually becoming conscious of the issue of data protection, the republic is seeing a proliferation in voluntary protection schemes. This is not much different from the EU, where in my observations the first response to growing consumer concern over online privacy was also the adoption of privacy policies and codes of practice by websites wary of losing visitors.

In 1998, the National Internet Advisory Committee ('NIAC'), an expert advisory body of the Media Development Authority of Singapore, introduced an "E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce" ('E-Commerce Code').[53] The code had no official regulatory force, but it was soon adopted as part of a voluntary accreditation scheme called CaseTrust for consumer businesses.[54] CaseTrust has since been subscribed to by approximately a hundred businesses.[55]

Soon after the E-Commerce Code was adopted, the international influence of the *Data Protection Directive* became apparent. Unfortunately, the E-Commerce Code

---

47 *Supra* note 43.

48 *Supra* note 10, Annex 2, at 42-45.

49 For an example of a statute of the latter type from the list referred to in the previous note, see *Science Centre Act* (Cap. 286, 1985 Rev. Ed. Sing.)

50 See text accompanying *infra* note 109.

51 Michael Hwang & Andrew Chan, *supra* note 14 at 355.

52 *Ibid.*

53 National Internet Advisory Committee, "Annual Report 1997-1998" (1999) at 15-19, Annex A, online: MDA. <http://www.mda.gov.sg/MDA/documents/Report_ NIAC_1997 _1998.pdf>.

54 *Supra* note 10 at 8.

55 As at December 2004. See CaseTrust companies list, online: Consumers Association of Singapore <http://www.case.org.sg/casetrust4.htm>.

was not designed to cope with the adequacy requirements of this *Directive*. Thus, NIAC set to work on drafting a new code that would comply with the requirements.[56]

In February 2002, NIAC Legal Subcommittee presented the new code, entitled the NIAC Model Code.[57] It is partly based on the Canadian Standards Association's Model Code for the Protection of Personal Information ('CSA Model Code'),[58] adopted in 1996. The CSA Model Code is in turn based on the 1980 OECD Guidelines.[59] In some parts, the NIAC Model Code also relies on the *Data Protection Directive* and the U.K. *Data Protection Act 1998*.[60] The NIAC Model Code is not focused solely on electronic commerce; it was the first code designed to be sector independent.

After the NIAC Model Code was released, IDA and National Trust Council ('NTC') conducted a public consultation on it. The consultation process resulted in a modified version entitled the Model Data Protection Code,[61] published in December 2002 ('MDPC'). This new code is now in use in a voluntary co-regulation data protection scheme.[62] The scheme is coordinated by the NTC, a co-operation between the government and the industry, set up for the purpose of promoting confidence in electronic commerce. According to the scheme, the NTC evaluates and nominates companies to act as Authorised Code Owners. The Authorised Code Owners then engage in the business of evaluating other voluntary companies and awarding them accreditations when they fulfil certain criteria. Awarded companies display these accreditations on their storefronts and web pages in the hope of winning consumer confidence and attracting business.[63] In this way, the MDPC now has a quasi-official status and in a way represents the best Singapore has to offer in the field of data protection.

In addition to the dominant NTC scheme and the MDPC, there are a number of other non-law instruments that contain some data protection elements. They include the Singapore Code of Advertising Practice[64] and the Code of Practice of the National Association of Travel Agents of Singapore.[65] In the telecommunications sector there is the IDA Code of Practice, which is actually quite forceful as operators

---

56 *Supra* note 10 at 9.

57 *Supra* note 10 at 21.

58 Canadian Standards Association, "Model Code for the Protection of Personal Information" (CSA-Q830-96, March 1996; reaffirmed 2001), online: Canadian Standards Association <http://www.csa.ca/standards/privacy/code/Default.asp?language=English>.

59 OECD, *Recommendation of the Council Concerning Guidelines on Governing the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980), 20 I.L.M. 422 (1981), online: The European Commission, Data Protection <http://europa.eu.int/comm/internal_market/privacy/instruments/ocdeguideline_en.htm>.

60 *Supra* note 34.

61 National Trust Council, "Model Data Protection Code" (December 2002), online: TrustSg <http://www.trustsg.com/radiantrust/tsg/rel1_0/html/downloads/Data_Protection_Code_v1.3.pdf> [*MDPC*].

62 I call this light-touch co-regulation, though it is not much different from pure self-regulation, where companies not only voluntarily subscribe to a code, but also come up with the contents of the code themselves. In this scheme, however, the government is involved, most prominently in the form of the Infocomm Development Authority.

63 The "TrustSg" scheme is explained in detail online: TrustSg <http://www.trustsg.org/>.

64 *Supra* note 14 at 371; *supra* note 43 at 8.

65 *Supra* note 43 at 8.

must abide by it to retain their license.[66] All of these codes are, however, limited to their respective sectors.

III. The Assessment Framework

Considering the purpose of this article, the method of assessing the Singaporean data protection regime must resemble as closely as possible the method applied by the EU. Article 25(6) of the *Data Protection Directive* provides that the European Commission has the power to make a decision of adequacy. To help the Commission perform its duties under the *Directive*, Article 29 establishes a Working Party. The Article 29 Data Protection Working Party ('Working Party') is an expert body composed of representatives from the data protection authorities of Member States.

One of the tasks of the Working Party is to "give the Commission an opinion on the level of protection in the Community and in third countries".[67] It is also required to "draw up an annual report […] regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission".[68]

When the Commission wishes to make a finding of adequacy, it first consults the Working Party. The Working Party then carries out an assessment of the data protection regime of the country in question, and the Commission acts on that advice. An Advisory Committee representing the Member States has the right to interfere,[69] but so far it has not challenged the opinions of the Working Party. This process has been followed in making the adequacy decisions concerning Argentina, Hungary and Switzerland.[70]

An exception to this process has been the case of U.S. Department of Commerce's Safe Harbor Privacy Principles ('Safe Harbor')[71], where the Commission made a positive finding regardless of some concerns expressed by the Working Party.[72] However, the finding in question is not a "blanket acceptance", and the exceptional arrangement will also be reviewed again when fully implemented to ascertain that the adequacy requirements are met. Similarly, the Canadian *Personal Information*

---

66 *Code of Practice for Competition in the Provision of Telecom Services* (S.412/2000 Sing.), online: Infocomm Development Authority of Singapore <http://www.ida.gov.sg/idaweb/doc/download/I488/Telecom_Competition_Code_2000.pdf>. Section 3.2.6 of the *Code* limits the use of end user service information.

67 *Data Protection Directive*, art. 30(1)(b), *supra* note 3.

68 *Data Protection Directive*, art. 30(6), *ibid*.

69 *Data Protection Directive*, art. 31, *ibid.*

70 EC, *Commission Decision C(2003)1731 of 30 June 2003* [2003] O.J. L. 168/19; EC, *Commission Decision C(2000)2305 of 26 July 2000* [2000] O.J. L. 215/4, 25.8 and EC, *Commission Decision 2000/518/EC of 26 July 2000* [2000] O.J. L. 215/1 respectively.

71 United States Department of Commerce, "Safe Harbor Privacy Principles" (21 July 2000), online: U.S. Department of Commerce Export Portal <http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm> [*Safe Harbor Privacy Principles*]. The associated "F.A.Q." and other documents are available online: <http://www.export.gov/safeharbor/>.

72 See EC, *Commission Decision 2000/520/EC of 26 July 2000* [2000] O.J. L. 215/7. For the concerns expressed by the Working Party, see EC, *Data Protection Working Party, Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"*, CA07/434/00/EN—WP 32 (16 May 2000) at 7-8, online: The European Commission, Data Protection <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp32en.pdf>.

Protection and Electronic Documents Act ('*PIPEDA*')[73] was approved despite certain milder reservations expressed by the Working Party. Safe Harbor and *PIPEDA* are discussed more later in this article.

Notwithstanding the political dimension that sometimes affects the Commission's findings, this article will try to mimic as closely as possible the method used by the Working Party. Most conveniently, the Working Party has discussed its methods explicitly in several adopted documents:

1. *Discussion Document: First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy*;[74]
2. *Working Document: Judging industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country?* ('WP 7');[75]
3. *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* ('WP 12').[76]

A. *The WP 12 Framework*

WP 12 is the latest and most comprehensive of these documents. It describes a complete framework of substantive requirements that a given data protection regime must fulfil. In terms of detail and applicability, this is a giant leap from Article 25(1), which simply calls for an "adequate level of protection." This framework is now the benchmark of adequate protection.

How did the Working Party arrive at this framework? It is not merely derived from the requirements set by the *Data Protection Directive* on Member States. As the Working Party observes, "there is a degree of consensus as to the content of data protection rules which stretches well beyond the fifteen states of the Community."[77] Accordingly, the framework seeks to encompass the core data protection principles established in a number of international legal documents: Council of Europe Convention No. 108 (1981);[78] OECD Guidelines (1980);[79] and the UN Guidelines (1990).[80] This reliance on international consensus serves to establish a level of legitimacy that a directive with such extra-territorial effects arguably needs.

The framework consists of two parts: *content principles* and *enforcement objectives*. According to the Working Party, they "constitute a 'core' of data

---

73 S.C. 2000, c. 5.

74 EC, *Data Protection Working Party,* DG XV D/5020/97—WP 4 (26 June 1997), online: The European Commission, Data Protection <http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_en.htm>. All the Article 29 Working Party documents cited in this paper are available at the foregoing address.

75 EC, *Data Protection Working Party,* DG XV D/5057/97—WP 7 (14 January 1998), online: *ibid.*

76 EC, *Data Protection Working Party,* DG XV D/5025/98—WP 12 (24 July 1998), online: *ibid* [*WP 12*].

77 *WP 12*, *ibid.* at 5.

78 *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981, Eur. T.S. No. 108 (entered into force on 1 October 1995).

79 *Supra* note 59.

80 UN OHCHR, *Guidelines for the Regulation of Computerized Personal Data Files*, UN GA Res. 45/95 (14 December 1990), online: Office of the High Commissioner for Human Rights <http://www.unhchr.ch/html/menu3/b/71.htm>.

protection ... compliance with which could be seen as a minimum requirement for protection to be considered adequate."[81] Content principles specify minimum requirements for the content of rules governing all collection, processing and dissemination of personal data. Enforcement objectives are the principal performance goals of the mechanism used to enforce the substantive rules. There are six content principles that should be applied generally:

(1) the purpose limitation principle;
(2) the data quality and proportionality principle;
(3) the transparency principle;
(4) the security principle;
(5) the rights of access, rectification and opposition; and
(6) restrictions on onward transfers.[82]

Additional safeguards should be applied for types of processing which, by their nature, constitute an increased risk for the data subject. The framework identifies a non-exhaustive list of three additional content principles:

(1) special handling of sensitive data;
(2) possibility to 'opt-out' from direct marketing; and
(3) special rules for automated individual decision making.[83]

The three enforcement objectives are:

(1) to deliver a good level of compliance with the rules;
(2) to help data subjects in the exercise of their rights; and
(3) to provide appropriate redress for the injured party where the rules are not complied with.[84]

The exact content of the principles and the objectives and their correct application is discussed in more detail on a rule-by-rule basis in the following two parts of this article. I refer to a number of other Working Party documents, which clarify and elaborate on the views of the Working Party. Of particular relevance is the Working Party's opinion on the Canadian *PIPEDA*, because the Act is based on the same CSA Model Code that underlies parts of the Singaporean MDPC. I also make reference to the *Data Protection Directive* where it is the intention of the Working Party that provisions of the *Directive* be imposed on third countries, or when it is otherwise necessary for the correct interpretation of the framework. However, what is said in the *Directive* cannot generally be understood to be a direct requirement for third countries.

A final note concerning the framework: Within the European Community, data protection regimes are, without exception, incorporated in law. However, this is not necessarily the case in third countries. In Singapore, there are sector-specific data protection laws and some privacy protections included in other laws, but no omnibus data protection law. The MDPC has a more general scope of application, but it is a

---

81 EC, *Data Protection Working Party, Opinion 4/2002 on adequate level of protection of personal data in Argentina*, 11081/02/EN/Final—WP 63 (3 October 2002), online: *supra* note 74 [*Argentina Opinion*].
82 *WP 12*, *supra* note 76 at 6.
83 *WP 12*, *supra* note 76 at 7.
84 *WP 12*, *supra* note 76 at 6.

voluntary code of conduct, not a statute. Is the Code to be taken into consideration when assessing the adequacy of Singapore's data protection regime under Article 25? The Code, when adopted, amounts to self-regulation on the part of the data controller. It is also incorporated into a co-regulation scheme. Article 25(2)[85] states that "[t]he adequacy […] shall be assessed in the light of all the circumstances surrounding a data transfer operation" and that consideration should be given to the "rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."

The Working Party reads this to include industry self- and co-regulation: chapter three of WP 12 deals with assessing industry self-regulation as a part of the protection regime, and the Working Document "*Judging industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country?*"[86] deals with the same matter. Industry self-regulation and codes of conduct are definitely within the scope of the framework, so that they must be taken into account when assessing the adequacy of a regime. But as is shown in the next part, they may not go a very long way towards fulfilling the WP 12 criteria.

IV. Adequacy of Scope, Processes and Enforcement Mechanisms

Having described the state of data protection in Singapore, and what the EU expects an adequate protection regime to deliver, I now begin comparing these two standards against each other to see how the Singaporean data protection regime measures up. I start by assessing the scope, processes and enforcement mechanisms, because the recommendations I make in relation to them enable me to make a useful assumption later when I move on to examine the substantive rules.[87]

A. *Scope*

The scope or reach of a regime can be broken down to a number of dimensions. The Working Party has used the following division:[88] (1) scope with regard to the data controller, (2) scope with regard to the data subject, (3) scope with regard to the means of processing, (4) scope with regard to the purpose of the processing operations, and (5) territorial scope.[89]

1. *Scope with regard to the data controller*

Ideally, when a country is found to provide adequate protection under Article 25, all data flows from EU Member States to that country are thereafter automatically

---

85 *Data Protection Directive*, *supra* note 3.

86 *WP 7*, *supra* note 75.

87 See heading "*V. Adequacy of substantative rules*" below.

88 See for example the *Argentina Opinion*, *supra* note 81 at 4-7.

89 When assessing Argentina and Switzerland, the Article 29 Working Party had to take into account the fact that those countries have federal constitutions, so that data protection laws could differ from one part of the country to another. This is obviously not an issue in Singapore, so we forego territorial scope in the following analysis.

assumed to be adequately protected, regardless of what entity the recipient within that jurisdiction is. For this to make sense, the data protection rules of that country must apply to all entities, all data controllers within the jurisdiction: public or private, corporate and individual, actual and potential.

However, as indicated in Article 25(2) and demonstrated by the Commission's acceptance of the U.S. Safe Harbor arrangement[90] and the Canadian *PIPEDA*,[91] regimes that apply only to a limited set of data controllers may also be acceptable. Thus it is possible to entertain the thought that the National Trust Council accreditation scheme, which only applies to those organisations that voluntarily subscribe to it, could ask for a positive finding from the EU Commission even if the rest of Singapore could not meet the standard. In this case, the free flow of information from the EU would apply only to the organisations participating in the scheme.

As to the other data protection instruments in Singapore, the scope of the various statutory data protection rules extends to different public sector bodies and some industries in the private sector. The common law torts discussed have more or less universal application within the jurisdiction, subject to their own rules.

2. *Scope with regard to the data subject*

The *Directive* requires only that personal data transferred to the third country from a EU Member State be protected.[92] It seeks to protect the privacy of EU citizens and does not try to prescribe how other governments should protect their own. However, for a number of reasons, most countries have chosen to treat all data subjects equally, regardless of nationality or source of data flow.[93] There are moral reasons, in my opinion, but also very practical ones: in many cases, it could be difficult or impossible to determine the nationality of a data subject whose data is being automatically processed; it could be costly for data controllers to implement systems that differentiate between data subjects; and it could be difficult to enforce such a regime.[94] Taking heed of these facts, the MDPC applies to all data subjects regardless of nationality. The statutes and the common law also generally protect subjects without regard to nationality.[95]

3. *Scope with regard to the means of processing*

The MDPC applies to all processing of personal data, "whether or not by electronic means".[96] However, personal data is defined as being in electronic form. It follows

---

90 EC, *Commission Decision 2000/520/EC of 26 July 2000* [2000] O.J. L. 215/7.

91 EC, *Commission Decision 2002/2/EC of 20 December 2001 on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act* [2002] O.J. L. 2/13.

92 Though whether the data concerns EU citizens or citizens of other countries does not make a difference.

93 This applies to data subjects that are natural persons; protection of other legal persons varies. The EU *Data Protection Directive*, *supra* note 3, and this article are concerned exclusively with the protection of natural persons.

94 *Supra* note 10 at 54.

95 See Looi Teck Kheong, *supra* note 14, for arguments supporting the enactment of data protection legislation in Singapore.

96 *MDPC*, s. 1.3, *supra* note 61.

that the MDPC does not apply to *e.g.* manual filing systems. The EU *Data Protection Directive*, on the other hand, applies to electronic processing as well as "to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."[97] When evaluating the U.S. Safe Harbor regime, the Working Party indicated that it would require third countries to meet this standard.[98]

However, the Commission[99] seems to have disregarded the Working Party in this instance, because it granted approval to Safe Harbor anyway, despite the fact that it excludes manual filing systems from protection.[100] This reflects the slight 'political dimension' of the adequacy findings mentioned above.[101] Singapore could either try to follow this precedent or play it safe and amend the rules to include manual filing systems.

4. *Scope with regard to the purpose of processing operations*

The MDPC is designed to apply to all processing of personal data regardless of purpose, subject to a number of exceptions.[102] The exceptions concerning personal use, journalistic, artistic and literary purposes, research and statistical purposes, national security and law enforcement should be acceptable: the EU *Data Protection Directive* contains very similar exceptions,[103] and the Working Party has approved of similar exceptions in its past opinions.[104]

Exception 1.2(d)[105] exempts "[p]rocessing by any organisation directly relating to a current or former employment relationship between the organisation and the individual." The treatment of employment data is a complex issue and has been the subject of considerable debate in the EU and Member States. However, to the extent that employment data matches the definition of personal data, it falls under the *Data Protection Directive* without question. The Working Party has confirmed this and is of the opinion that third countries must protect such employment data like any other personal data to be considered as providing an adequate level of data protection.[106]

B. *Processes and Enforcement Mechanisms*

In Europe, data protection regimes are embodied in law, so they automatically benefit from the processes and mechanisms associated with enforcing law and providing

---

97 *Data Protection Directive*, art. 3(1), *supra* note 3.

98 EC, *Data Protection Working Party, Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government*, 5092/98/EN/final—WP 15 (26 January 1999), online: *supra* note 74.

99 *Supra* note 72.

100 *Safe Harbor Privacy Principles*, *supra* note 71 at 2.

101 See text accompanying *supra* note 72.

102 *MDPC*, s. 1.2, *supra* note 61.

103 See for example Article 9.

104 See for example the *Argentina Opinion*, *supra* note 81 at 6-7.

105 *Data Protection Directive*, s. 1.2(d), *supra* note 3.

106 EC, *Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context*, 5062/01/EN/Final—WP 48 (13 September 2001) at 4, 26, online: *supra* note 74. In the same document the Working Party shows why the diligent protection of employment data does not impose an onerous duty on the employer, in a large part thanks to certain flexibilities in the *Directive*.

remedy for breaches. EU member states also provide additional ways and means in the form of a national data protection authority. A data protection authority complements and strengthens the legal regime by informing and educating data subjects and data controllers, by providing additional light-weight processes through which disputes may be investigated and settled outside the judiciary, and by generally ensuring that the laws are observed.

However, data protection law is the means, not the end. The Working Party recognised that other jurisdictions may seek to implement substantially equivalent data protection measures in formally different ways. To avoid prejudicing any system, the Working Party identified certain objectives that any adequate regime must meet regardless of how it is implemented.[107] Thus the Singaporean tapestry of data protection is examined in light of these objectives:

1. *Objective 1*

Objective 1 is defined as:

> To deliver a good level of compliance with the rules. (No system can guarantee 100% compliance, but some are better than others.) A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.[108]

The Working Party is aware that a "good level of compliance" may be subjective and hard to quantify. Therefore the definition provides a list of secondary indications of a high-compliance system. I proceed to examine whether the Singapore system exhibits these characteristics.

As the NIAC stated after examining the present state of data protection in Singapore, "A proliferation of data protection regimes and practices is confusing to consumers."[109] Singaporean consumers in general are certainly not aware of the legion of voluntary codes, statutes and common law remedies that could potentially protect some aspects of their privacy and personal data. It would be even more difficult for European consumers. The level of awareness among data controllers is less clear, but it seems probable that the multi-faceted system is confusing to them as well. As to verification by authorities, auditors and officials, the NIAC also observed that a "diversity of data protection regimes also makes monitoring and auditing by the relevant authorities difficult."[110]

The National Trust Council's ('NTC') MDPC based co-regulatory scheme has potential in this respect. Currently only a small fraction of companies in Singapore have sought accreditation under the scheme, but the NTC is trying to position the scheme as having a wide participation in the future. If a single scheme was to become overwhelmingly popular, reaching almost as wide as an omnibus law, then

---

[107] *WP 12*, *supra* note 76 at 7.
[108] *Ibid.*
[109] *Report On A Model Data Protection Code*, *supra* note 10 at 14.
[110] *Ibid.*

most of the problems associated with a fragmented regime would disappear. However, NTC and the two Authorised Code Owners, CommerceNet Singapore Pte. Ltd. (ConsumerTrust Global Reliability Programme) and the Consumers' Association of Singapore ('CASE') (CaseTrust), are at the moment not doing the best possible job at promoting "awareness [...] among data subjects of their rights and the means of exercising them."

Both CommerceNet and CASE argue on their respective websites that any company displaying the mark of accreditation is abiding by the Code of Practice, and should therefore be trusted by consumers as providing a good level of data protection, among other things.[111] However, neither company makes their Code of Practice available on their website, although they do provide brief summaries.[112] To put it bluntly, they expect consumers to trust their marks without giving details as to what exactly the marks stand for.

The NTC website[113] states that an "ACO [Authorised Code Owner] will assess [the company's] business practices guided by the TrustSg Core Principles for businesses conducted electronically." The TrustSg Core Principles[114] encompass the MDPC. Principle 3, entitled "Data Protection", duplicates the Code verbatim. In other words, an assessment of the company will be "guided" by the MDPC, but is the company obliged to live up to the standard set in the MDPC? If CaseTrust still uses the NIAC E-Commerce Code like they did in 2001,[115] then their actual data protection requirements are considerably less stringent than the MDPC's. Whatever the truth, this shows that the current state of affairs is certainly confusing to a data subject, and perhaps so for a data controller as well. Finally, a NTC self-assessment checklist for merchants is marked "confidential" on every page.[116] This seems symbolic of the scheme's current level of devotion to openness.

2. *Objectives 2 and 3*

Objective 2 is defined as:

> To provide support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.[117]

---

[111] The Consumers' Association of Singapore's CaseTrust website can be found at <http://www.ct.case.org.sg/>. CommerceNet's website is at <http://www.commercetrust.com.sg/>.

[112] CommerceNet produced their Code of Practice promptly when it was requested via e-mail. It turns out that their Code of Practice equals the Model Data Protection Code. CaseTrust did not respond to e-mailed requests for their Code of Practice. According to an "infokit" available on their website, the full criteria will be made available to a company upon submission of an application fee of S$120.

[113] <http://www.trustsg.com/>.

[114] TrustSg Core Principles Version 7.0 (August 2003), online: TrustSg <http://www.trustsg.com/radiantrust/tsg/rel1_0/html/downloads/TrustSg_Core_Principles_V7.0.pdf >.

[115] *Report On A Model Data Protection Code*, *supra* note 10 at 8.

[116] The checklist is available online: <http://www.trustsg.com/radiantrust/tsg/rel1_0/html/downloads/Self_Assessment_for_Merchants.doc>

[117] *WP 12*, *supra* note 76 at 7.

Objective 3, related to same issues, is defined as:

> To provide appropriate redress to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.[118]

Any data protection rules incorporated in the statutes and common law torts discussed above[119] come with their associated legal processes and remedies. In other words, a dissatisfied individual may sue a data controller. Judicial review is certainly independent and its result enforceable, but litigation is by no means a rapid or inexpensive way to resolve data protection complaints.

As to the NTC's co-regulatory scheme, the lack of information concerning the exact content of the data protection rules makes it difficult for a data subject to make a claim.[120] Assuming that a data subject does make a claim, the MDPC in itself only provides for a system where the data controller itself addresses the claim. The implementation of the system is left for the data controller and the paying of compensation is not explicitly required. There is no help or support offered to the individual in the exercise of his claims.

The Authorised Code Owners amend this scheme significantly by making independent mediation services available to the claimant and the accredited company if the first step described above should fail.[121] However, the mediation is voluntary and it does not result in a decision or judgment being passed. The only outcome can be an agreement between the claimant and the company, save perhaps that the company may lose its right to display the mark of accreditation.

For sanctions to be imposed on a party or compensation to be extracted beyond what the party is agreeable to, the claim must be taken to the Small Claims Tribunal or some other suitable court. But this is only possible if the claimant has a valid claim under some law. A breach of the voluntary data protection scheme might not suffice, unless it can somehow be fashioned as a breach of contract. In any case, at this point the process is well beyond providing a rapid and inexpensive remedy. The mediation services offered by the ACOs are not free, either. CommerceNet charges S$50 per party, while CaseTrust has a more complicated pricing scheme that takes into account the value of the claim.[122] To access CaseTrust mediation, an individual must also first become a CASE member and pay the associated membership fees.[123]

C. *Recommendations*

It is clear that the present tapestry of data protection law cannot be considered adequate for reasons of both enforcement, considering the individual's ability to seek

---

[118] *Ibid.*

[119] See headings "*A. Common Law*" and "*B. Statutes*" above.

[120] See text accompanying *supra* note 116.

[121] CommerceNet's dispute resolution mechanism is described online: Consumer Trust Dispute Resolution Mechanism <http://www.commercetrust.com.sg/cst_dispute.htm>. CaseTrust's dispute resolution process is online: Consumers Association of Singapore <http://www.case.org.sg/medi1.htm>.

[122] A pricing chart is available online: Consumers Association of Singapore <http://www.case.org.sg/medi2.htm>.

[123] See CASE, "How to lodge a complaint?", CaseTrust dispute resolution process, online: *supra* note 121.

remedy, and scope, especially with regard to data controllers. In my view, the most efficient way to address these inadequacies would be to replace the current patchwork with a single omnibus regime. The NTC's co-regulatory scheme involving the MDPC is a move in this direction. However, it is inadequate on two dimensions of scope, namely the scope with regard to means of processing and the scope with regard to the purpose of processing operations, and should be amended accordingly.[124]

The co-regulatory scheme also falls short of providing adequate processes and enforcement mechanisms. Some of the issues could be addressed by improving openness and transparency in the organisations involved in regulating the scheme. Other problems could be addressed by ensuring that the companies are legally bound by the Codes of Practice, and are subject to the jurisdiction of a competent authority able to impose sanctions. The scheme could learn something from the U.S. Safe Harbor arrangement in this respect.[125]

If the MDPC-based scheme is successfully amended, then the scheme could in theory apply for a finding of adequacy by itself, regardless of the level of data protection present in Singapore in general. In practice this could be difficult, however. The U.S. Safe Harbor arrangement came to be only after considerable hardship and extended negotiations between the U.S. and the EU, and it can be questioned whether the EU would be willing to put similar effort into reaching an agreement with any other country.

Another problem with a limited finding of adequacy are the "boundary issues": data transfers between the EU and the accredited companies would be straightforward, but data transfers between the accredited companies and other non-accredited organisations in Singapore would become problematic. Thanks to Safe Harbor, this is now the state of affairs in the U.S., and it is interesting to see what comes of it in the future.

The recommended alternative to amending the co-regulatory scheme is to legislate: to enact a comprehensive data protection law, complete with a governmental data protection authority. This should be done carefully to address all the identified inadequacy pitfalls of scope, process and enforcement. The substantive content of the law could be based on Singapore's current leading data protection document, the MDPC, because it already enjoys a level of recognition in the island republic. But the MDPC needs to be amended first. Thus in the next part I examine the substantive content of the Code and lay the rest of the tapestry to rest.

V. Adequacy of Substantive Rules

In this part, I make the assumption that the MDPC has been incorporated into an omnibus data protection law, as was done with the CSA Model Code in Canada. The law covers all sectors, public and private alike. Even though substance and enforcement can never be completely separated from each other, in this scenario

---

[124] See headings "*3. Scope with regard to the means of processing*" and "*4. Scope with regard to the purpose of processing operations*" above.

[125] Safe Harbor is not a perfect example, as it has attracted criticism even from the Article 29 Working Party, but it does subject participating companies to the mandatory jurisdiction of the U.S. Federal Trade Commission. See *Safe Harbor Privacy Principles*, *supra* note 71, para. 3.

it is reasonable to assume that compliance is high. Thus I proceed to assess the substantive rules of the Code based solely on their wording.

As established in Part III,[126] to be seen as offering an adequate level of protection, the provisions of the MDPC must satisfy the Working Party principles. Other elements of the prevailing data protection regime must also be taken into account, but it is difficult to see how they could help in filling possible gaps in the MDPC. All of the laws and codes listed in Part II are limited in scope in one way or the other, while the data protection principles we are looking at here are applied generally, without regard to the identity of the data subject or the organisation, or to the type of personal data (except where indicated below).

Annex 1 to this article contains a table of comparisons between the Working Party principles and the relevant sections of the Code.[127] The principles and any closely related articles of the *Data Protection Directive* are listed in the left column. Sections of the Code which were considered to be relevant to a given principle are quoted in the corresponding row in the right column. Below is a principle-by-principle breakdown of what the juxtaposition reveals about the adequacy of the Code, and recommendations on how to amend it where inadequate.

Note that while the Working Party documents and the MDPC share a lot of terminology, not all words are used in the exact same meaning. The Code defines its key terms in section 2. The Working Party documents for the most part do not define terms, but it is reasonable to assume that they follow the definitions established in Article 2 of the *Data Protection Directive*. Notable differences are highlighted below.

A. *The Purpose Limitation Principle*

> [D]ata should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.[128]

In the language of the *Directive*, "processing" includes not only all forms of use, alteration and adaptation, but also all collection, recording, dissemination and disclosure.[129] The purpose limitation principle therefore has a wide meaning. Nevertheless it is mirrored in Sections 4.4 and 4.5 of the Code: *Limiting Collection* and *Limiting Use, Disclosure and Retention*. Section 4.4 limits the collection of personal data "to that which is necessary for the purposes specified by the organisation." Section 4.5 limits the use, disclosure and retention in an equal way. Sections 4.4 and 4.5 contain a number of exceptions to the limitation. The Working Party principle also refers to a number of exceptions listed in Article 13 of the *Directive*. For the Code to qualify, Sections 4.4 and 4.5 exceptions should not be considerably wider or otherwise exceed the exceptions allowed for in Article 13.

---

[126] See heading "*III. The Assessment Framework*" above.

[127] Divisions in the *MDPC* are in fact also called principles, but to avoid confusion (and to reflect the fact that the Code is assumed to be law), this paper uses the word 'section' to refer to parts of the Code. The word 'principle' always refers to the principles listed in *WP 12*, *supra* note 76.

[128] *WP 12*, *supra* note 76 at 6.

[129] *Data Protection Directive*, art. 2(b), *supra* note 3.

One of the exceptions in Sections 4.4 and 4.5 concerns publicly available information. Under the exception, the collection and use of data that is "generally available to the public" does not need to be limited to any specified purpose.[130] The data may also be subsequently disclosed to third parties, if it is "generally available to the public in that form".[131]

It has been argued that what is already publicly available cannot be very sensitive or revealing, and thus there is no potential for injury, and no need for data protection. However, in my view the most prominent concern in computerised processing of personal data arises from aggregation. Thanks to efficient collection, processing and transfer of data between organisations, it is possible to aggregate mundane snippets of non-sensitive data into databases that reveal a great deal about a person and her lifestyle. This issue is much more complicated than that of regulating data that possesses a private character by itself.[132]

The protection of publicly available data was discussed in the EU when a Commission paper[133] and a subsequent directive[134] encouraged making public sector information databases publicly available in the Member States to achieve convenience for citizens and value for businesses. It was then held that when such information constitutes personal data, the usual rules of data protection apply. The Working Party said: "It is perfectly clear from the wording of our data protection legislation that it applies to personal data made publicly available [...] The principle of purpose requires that personal data are collected for specific, explicit and legitimate purposes and are not subsequently processed in a manner which is incompatible with these purposes."[135]

In the context of third countries, the Working Party touched on the issue of publicly available data when evaluating the Canadian *PIPEDA*.[136] *PIPEDA* permits the collection, use and disclosure without knowledge or consent of the individual of publicly available information when it "is specified by the regulations."[137] The regulations specify five categories of information, which encompass typical public sources such as telephone directories and advertisements.[138]

The Working Party remarked on this exemption, but accepted it, stressing that the regulations place restrictions on the secondary uses of the information.[139] Even though knowledge and consent is not required, any collection, use and disclosure

---

130 *MDPC*, ss. 4.4(d), 4.5(d), *supra* note 61.

131 *Ibid.*, s. 4.5(m).

132 Though publicly available data of a more sensitive character may become a bigger issue in the future, as access is made easier and more efficient. For example, a searchable case law database on the Internet could be used to instantly find court cases relating to a specific individual.

133 EC, *Public Sector Information: A Key Resource for Europe*, Com(1998)585, online: European Commission <http://europa.eu.int/information_society/topics/multi/psi/docs/pdfs/green_paper/ gp_en.pdf>.

134 EC, *Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information* [2003] O.J. L. 345/90.

135 EC, *Data Protection Working Party, Opinion 3/99 on Public sector information and the protection of personal data*, 5009/00/EN—WP 20 (3 May 1999) at 4, online: *supra* note 74.

136 EC, *Data Protection Working Party, Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act*, 5109/00/EN—WP 39 (26 January 2001), online: *supra* note 74.

137 S.C. 2000, c. 5, ss. 7(1)(d), (2)(c.1), (3)(h.1).

138 *Regulations Specifying Publicly Available Information,* S.O.R./2001-7, Part II.

139 *Supra* note 136 at 4.

must still be in line with the original purpose of the information. The approach taken by the Code towards publicly available data might therefore need to be amended to gain approval from the Working Party.

The Canadian regulations also specify two "investigative bodies" for the purposes of certain exceptions to the purpose limitation principle in *PIPEDA*.[140] The Singaporean Code has adopted the same exceptions,[141] but as no corresponding regulations obviously exist, the "investigative bodies" remain undefined. This creates a somewhat vaguely defined gap to the purpose limitation principle, which is a possible compliance problem.

B. *The Data Quality and Proportionality Principle*

> [D]ata should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.[142]

Section 4.6 of the Code begins: "Personal data shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used." Sections 4.4 and 4.5, as discussed above, are designed to prohibit excessive collection and processing. The Code thus satisfies this principle squarely.

C. *The Transparency Principle*

> [I]ndividuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the directive.[143]

Section 4.8 of the Code, entitled "Openness", obliges the data controller to "make readily available" specific information concerning the identity of the controller, its policies or standards, and the types of data held, including "a general account of their use". Section 4.2 is concerned with specifying the precise purposes of the processing. It states that the purposes shall be "specified", meaning that the data controller shall specify the purposes for its own internal use. Subsection 4.2.2 goes further by stating that the "purposes should be specified to the person from whom the personal data is collected or to the individual".

I see two potential problems with subsection 4.2.2. As the language of the subsection is not prescriptive, disclosure of the purposes under the Code is actually wholly optional.[144] This would not seem adequate in light of the wording of the principle. However, the same type of language was accepted without comment in *PIPEDA*, which I take to mean that the issue is not fatal. A second small compliance issue is

---

[140] S.C. 2000, c. 5, s. 7(3)(d), (h.2).

[141] *MDPC*, ss. 4.5(j), (n), 4.9(b), *supra* note 61.

[142] *WP 12*, *supra* note 76 at 6.

[143] *Ibid.*

[144] "Clauses which use prescriptive language (*i.e.* the words 'shall' or 'must') are requirements. The use of the word 'should' indicates a recommendation.": *MDPC*, *supra* note 61 at 5.

that the Code allows the purposes to be disclosed to an intermediary who provides the data ("person from whom the data is collected") instead of the data subject. Under the principle, the purposes must be disclosed to the data subject. *PIPEDA* takes this approach, too. Thus 4.2.2 seems inadequate, unless it is amended to ensure that the intermediary then communicates the purposes to the individual.[145]

D. *The Security Principle*

> [T]echnical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.[146]

Section 4.7 of the Code, entitled "Safeguards", states that "Personal data shall be protected by appropriate safeguards." Subsection 4.7.1 obliges organisations to protect data against unauthorised access amongst other things. The Code would thus seem to satisfy the security principle.

E. *The Rights of Access, Rectification and Opposition*

> [T]he data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.[147]

Section 4.9 of the Code, entitled "Individual access and correction", corresponds roughly to this Working Party principle. There is a minor issue with the circumstances in which the organisation must not or may choose not to comply with the data subject's requests: Exception (b) grants investigative bodies and government authorities a right to veto certain requests issued by individuals to organisations. As mentioned above,[148] the "investigative bodies" are undefined, leading to ambiguity. While the *PIPEDA* contains the same exception, it defines the investigative bodies in corresponding regulations.

F. *Restrictions on Onward Transfers*

> [F]urther transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (*i.e.* the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive.[149]

---

145 This is the method adopted by the *Data Protection Directive*, art. 10 and 11, *supra* note 3.
146 *WP 12*, *supra* note 76 at 6.
147 *Ibid.*
148 See text accompanying *supra* note 141.
149 *WP 12*, *supra* note 76 at 6.

Restrictions on onward transfers are a main focal point of the framework. Were such restrictions not in place, organisations could undermine the whole regime by transferring personal data away from the jurisdiction of the regime for unlimited use and disclosure. The corresponding section in the MDPC is 4.1.1:

> Where data are to be transferred to someone (other than the individual or the organisation or its employees), the organisation shall take reasonable steps to ensure that the data which is to be transferred will not be processed inconsistently with this Model Code.

Section 4.3 also requires, subject to several exceptions, that consent (explicit or implicit) be obtained from the individual before personal information can be disclosed to third parties.

In my view, Section 4.1.1 is not as rigorous as the Working Party principle. The analysis is as follows: The Code places an obligation on the originating organisation when a transfer takes place. In contrast, the principle operates from the assumption that no transfer shall take place unless the recipient of the transfer satisfies certain criteria. The obligation borne by the originator under the Code might not be especially exacting, while under the principle, the condition must be met or there shall be no transfer. Under the Code, data subjects would have no remedy as long as the originator made a "reasonable" attempt to ensure protection, while the principle could possibly give rise to strict liability.

Nevertheless, the Canadian *PIPEDA*, approved by the Commission, has similar provisions for restricting onward transfers.[150] The Working Party was not entirely satisfied with those provisions, though, opining "the transfer of data outside Canada would require the use of contractual or other binding provisions able to provide a comparable level of protection".[151] Obtaining consent from the individual is a legitimate way to enable an onward transfer without adequate protections, but if obtaining such consent becomes a common practice whenever information is collected, it is in my view questionable how informed that consent is. An explicit reference to binding contractual arrangements would be better from the point of view of privacy. In Europe, the Commission and the national privacy commissioners have taken it upon themselves to facilitate such arrangements.[152]

It is worth noting that the original NIAC Model Code, which the MDPC is a derivative of, had a separate section titled "Transborder Data Flows". The section was inspired by the *Directive*, which in a way takes a country-centric approach to regulating onward transfers. If the MDPC was incorporated in law and applied to all organisations in Singapore, this could be a sensible approach for the Code too.

---

[150] S.C. 2000, c. 5, Schedule I, 4.1.3, 4.3.

[151] *Supra* note 136 at 5-6.

[152] The Commission has published standard contractual clauses that help organisations implement such arrangements efficiently. Privacy commissioners provide organisations with advice and assistance. See "Model Contracts for the transfer of personal data to third countries", online: European Commission, Data Protection <http://europa.eu.int/comm/internal_market/privacy/ modelcontracts_en.htm>.

G. *Sensitive Data*

In addition to the six main principles, there are three additional principles that apply in specific circumstances. The first relates to sensitive data:

> [W]here 'sensitive' categories of data are involved (those listed in article 8 of the directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.[153]

Sections 4.3 and 4.7 of the Code, entitled "Consent" and "Safeguards" respectively, instruct organisations to place additional safeguards on data that must be considered sensitive, the level of the safeguards depending on the sensitivity of the data. However, the language is not precise nor prescriptive, and thus no specific obligations relating to the safeguards are introduced. Explicit consent is merely recommended, but not required. *PIPEDA* has very similar provisions for dealing with sensitive data. The Working Party remarked slightly on their ambiguity, adding that it would prefer a "systematic use of highest level of protection when sensitive data is processed and encourages the Canadian authorities and in particular the Privacy Commissioner to work towards this goal."[154]

Regarding what data is to be considered sensitive, the Code adopts a flexible approach. "Although some data (for example, medical records and income records) are almost always considered to be sensitive, any datum can be sensitive, depending on the context."[155] A helpful example concerning subscription to a special interest magazine is given. This seems like a shrewd way to approach the problem of defining sensitive personal data.

In contrast, Article 8 of the *Data Protection Directive*, which the principle references, contains a specific list of categories of data that are to be considered sensitive: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.[156] Data relating to offences, criminal convictions, security measures, administrative sanctions, and judgments in civil cases is afforded a semi-sensitive status.[157] Member States are also instructed to consider limitations on the processing of national identification numbers or other identifiers of general application.[158]

Article 8 lacks the flexibility of the Code in defining sensitive data. However, when it comes to implementing this rule in organisations, the problem with the Code is that it would push the problem of definition (and indeed the power to define) to the organisations. In my opinion, this might be problematic from a compliance point of view. In EU Member States, it is the national privacy commissioner who elaborates on

---

153 *WP 12*, *supra* note 76 at 7.
154 *Supra* note 136 at 4.
155 *MDPC*, *supra* note 61 at 12.
156 *Data Protection Directive*, art. 8(1), *supra* note 3.
157 *Data Protection Directive*, art. 8(5), *ibid.*
158 *Data Protection Directive*, art. 8(7), *ibid*.

the statutory definition of sensitive when necessary.[159] This arrangement introduces some flexibility without risking compliance.

H. *Direct Marketing*

> [W]here data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.[160]

Section 4.3, entitled *Consent*, provides that personal data may only be used with an individual's consent. Subsection 4.3.7 further provides that the individual may withdraw the consent at any time, subject to legal or contractual restrictions. These provisions create an opt-out mechanism that applies to all forms of use, including direct marketing. However, there is an important exception to the rule: the collection and use of personal data without the individual's knowledge or consent is permitted when the data is collected from publicly available sources.[161] Contact details, including email addresses, usually fall into the category of publicly available data.[162] Therefore, in most cases, an individual will not be able to opt out from direct marketing under the Code.

In an opinion concerning the Australian *Privacy Amendment Act*,[163] the Working Party stated that "allowing personal data to be used for direct marketing without an opt-out being offered cannot in any circumstance be considered adequate."[164] To be seen as offering an adequate level of protection, the Code must thus be amended in this respect. It is also worth noting that many jurisdictions, including the EU, have gone even further and adopted *opt-in* mechanisms for electronic direct marketing in order to combat the growing problem of unsolicited commercial e-mail.[165]

I. *Automated Individual Decision*

> [W]here the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to

---

159 In the *Data Protection Act 1998*, *supra* note 34, "sensitive personal data" is defined in s. 2. s. 51 requires the commissioner to make statements to the public about "the operation of this Act, about good practice, and about other matters within the scope of his functions." As part of this duty, the commissioner will have to interpret the Act, including s. 2. Part V. of the Act also gives the commissioner certain powers to enforce the Act, which also requires interpretation. In time, these materials form a body of 'precedent', to which organisations seeking clarification can refer.

160 *WP 12*, *supra* note 76 at 7.

161 *MDPC*, s. 4.3(h), *supra* note 61.

162 See text accompanying *supra* note 137 for a description of how *PIPEDA* deals with publicly available data.

163 *Privacy Amendment (Private Sector) Act 2000* (Cth.).

164 EC, *Data Protection Working Party, Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN—WP 40 (26 January 2001) at 5, online: *supra* note 74.

165 "The use of automated calling systems … , facsimile machines … or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.": EC, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* [2002] O.J. L. 201/37, art. 13(1).

> know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.[166]

Article 15(1) clarifies this principle that the automated decision in question is a decision that "produces legal effects concerning [the data subject] or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." Automated decision-making is seen as detrimental to the individual's interests, because it leaves no room for interpretation, explanation or bargaining. EU Member States are required to place strict legal limits on such decision-making, but third countries are not asked to do as much. The safeguards referred to could include "arrangements allowing [the data subject] to put his point of view".[167] The MDPC contains no provisions directly relating to automated decision-making, but neither does the *PIPEDA*. The Working Party has not discussed this issue in its opinions, so presumably it is not viewed as highly important.

VI. Summary of Conclusions and Discussion

At present there is a myriad of statutes, common law torts and voluntary schemes providing some level of protection for personal data in Singapore. However, they are all limited in one way or the other, and do not constitute a comprehensive data protection regime, even if put together. Under such a complex system, it is also very difficult for data subjects to exercise their rights.

The light co-regulatory scheme coordinated by the NTC represents a first effort to build an omnibus data protection regime in Singapore. In theory, a voluntary scheme could apply for a finding of adequacy from the EU separately from the rest of the country. However, the NTC scheme currently has severe shortcomings in terms of scope, processes and enforcement mechanisms.

The substantive content of the co-regulatory scheme is based on the MDPC. An assessment of the Code reveals that it satisfies some of the EU requirements and fails to satisfy certain others. With reasonable amendments it could be brought into compliance.

To deal with the issues of scope, processes and enforcement mechanisms, and to ensure that data flows are unimpeded not only between countries, but also between organisations within Singapore, I recommend that comprehensive data protection legislation be adopted in Singapore. The substantive content of the legislation could be based on an amended version of the MDPC, since the Code already enjoys a degree of recognition in the republic.

Singapore currently has no data protection commissioner. In many countries, a dedicated data protection commissioner's office is tasked with providing guidance and promoting awareness among organisations and individuals. The commissioner may act as an authority in interpreting the law, ensuring that it is applied consistently and efficiently. There are indications that the Working Party tolerated some ambiguities in the Canadian *PIPEDA* because it believed in the Canadian Privacy

---

[166] *WP 12*, *supra* note 76 at 7.

[167] *Data Protection Directive*, art. 15(2)(a), *supra* note 3.

Commissioner's ability to resolve them in a way that upholds privacy.[168] Had organisations been left on their own devices in interpreting and applying the statute, a more detailed text would likely have been necessary.

Industry groups typically advocate a self-regulatory approach towards data protection, criticising comprehensive legislation as unsuited for the full gamut of industry environments. In my opinion there are no indications that a broadly framed *Directive*-compliant data protection statute would be inapplicable to some sectors, though more research would be useful. In some countries, the data protection commissioner coordinates a form of co-regulation based on the data protection legislation.

For example, in Australia and New Zealand, the commissioner may approve an industry code of practice which then replaces the statute-based data protection rules for that sector.[169] As long as the industry codes are required to uphold the same level of protection as the legislation, there is no reason why such a scheme could not obtain approval from the EU Commission. However, I would tend to argue against such arrangements, because a proliferation of different codes brings back the confusion and ambiguity that comprehensive legislation is intended to clear.

ANNEX 1

WP12 Basic Principles

Working Party Principles		Model Data Protection Code
1) The purpose limitation principle	**1) The purpose limitation principle** Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the *Directive*.	**4.2 Principle 2—Specifying Purposes** The purposes for which personal data are collected shall be specified by the organisation. **4.4 Principle 4—Limiting Collection** Except as provided below, the collection of personal data shall be limited to that which is necessary for the purposes specified by the organisation. Data shall be collected by fair and lawful means. **4.5 Principle 5—Limiting Use, Disclosure, and Retention** Except as provided below, personal data shall not be used or disclosed to a third party for purposes other than those for which it was collected, unless the individual consents to such use or disclosure. Subject to any applicable legal requirements, personal data shall be retained only as long as necessary for the fulfilment of those purposes.

(*Continued*)

[168] See *e.g.* text accompanying *supra* note 154.
[169] *Supra* note 10 at 49-50.

Working Party Principles		Model Data Protection Code
	Article 13—Exemptions and restrictions 1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others. 2. […]	Collection/use beyond purposes specified is permitted where: (a) All of the following apply: i) the collection/use is clearly in the interest of the individual; ii) it is impracticable to obtain the consent of the individual to that collection/use; and iii) if it were practicable to obtain such consent, the individual would be likely to give it. (b) Collection/use with the knowledge or consent of the individual would compromise the availability or the accuracy of the data where such collection/use pertains to an investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed; (c) Data is being collected/used in an emergency that threatens the life, health or security of a person; (d) Collection/use is of data which is generally available to the public; or (e) The individual consents to the collection/use.

(*Continued*)

Working Party Principles		Model Data Protection Code
		Disclosure beyond the purposes of collection is permitted where: (f) All of the following apply i) the disclosure is clearly in the interest of the individual; ii) it is impracticable to obtain the consent of the individual to that use; and iii) if it were practicable to obtain such consent, the individual would be likely to give it. (g) Disclosure is made to a solicitor representing the organisation; (h) Disclosure is necessary for the purposes of establishing, exercising or defending legal rights; (i) Disclosure is to a government agency that has made a lawful request for the data; (j) Disclosure is made, on the initiative of the organisation, to an investigative body appointed by the organisation, or to a government agency for investigative purposes; (k) Disclosure is made to a person who needs the data because of an emergency that threatens the life, health or security of a person; (l) Disclosure is made to an institution whose purpose is the conservation of records of historic or archival importance and disclosure is for such purpose; (m) Disclosure is of data which is generally available to the public in that form; or (n) Disclosure is made by an investigative body and the disclosure is reasonable for purposes related to the investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being or is about to be committed.

(*Continued*)

Working Party Principles		Model Data Protection Code
2) The data quality and proportionality principle	**2) The data quality and proportionality principle** Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.	**4.6 Principle 6—Accuracy** Personal data shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. **4.4 Principle 4—Limiting Collection** **4.5 Principle 5—Limiting Use, Disclosure, and Retention** [see above]
3) The transparency principle	**3) The transparency principle** Individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the *Directive*.	**4.8 Principle 8—Openness** An organisation shall make readily available information about its policies and procedures for handling personal data. **4.8.2** The information made available shall include— (a) the name/title and address of the person who is accountable for the organisation's policies and procedures and to whom complaints or inquiries can be forwarded; (b) the means of gaining access to personal data held by the organisation; (c) a description of the type of personal data held by the organisation, including a general account of their use; (d) a description of the organisation's policies or standards; and (e) what personal data are generally made available or are likely to be made available to other organisations, including related organisations such as subsidiaries. **4.2 Principle 2—Specifying Purposes** [see above] **4.2.2** The identified purposes should be specified to the person from whom the personal data is collected or to the

(*Continued*)

Working Party Principles		Model Data Protection Code
		individual ("the relevant party"). Depending upon the way in which the data are collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.
4) The security principle	**4) The security principle** Technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.	**4.7 Principle 7—Safeguards** Personal data shall be protected by appropriate security safeguards. **4.7.1** The security safeguards shall protect personal data against accidental or unlawful loss, as well as unauthorised access, disclosure, copying, use, or modification. Organisations shall protect personal data regardless of the format in which they are held.
5) The rights of access, rectification and opposition	**5) The rights of access, rectification and opposition** The data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the *Directive*.	**4.9 Principle 9—Individual Access and Correction** Subject to the following exceptions, an individual shall upon his request be informed of the existence, use, and disclosure of his personal data and shall be given access to that data. An individual shall be able to challenge the accuracy and completeness of his personal data and have them amended as appropriate. The reasons for denying access should be provided to the individual upon request.

(*Continued*)

Working Party Principles		Model Data Protection Code
	Article 13—Exemptions and restrictions 1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);	The organisation shall refuse the request where: (a) Providing access would be likely to reveal personal data about another person, unless —the said person consents to the access; or —the individual needs the information because a person's life, health or security is threatened, provided that where the data about the said person is severable from the record containing the data about the individual, the organisation shall sever the data about the said person and shall provide the individual access; or (b) An investigative body or government agency, upon notice being given to it of the individual's request, objects to the organisation's complying with the request in respect of its disclosures made to or by that investigative body or government agency;
	(g) the protection of the data subject or of the rights and freedoms of others. 2. Subject to adequate legal safeguards, in	The organisation may refuse the request where: (c) Data is protected by solicitor-client privilege; (d) It would reveal data that cannot be disclosed for public policy, legal,

(*Continued*)

(*Continued*)

Working Party Principles		Model Data Protection Code
	particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.	security, or commercial proprietary reasons, provided that where the personal data about the individual is severable from the record that cannot be disclosed for public policy, legal, security or commercial proprietary reasons, the organisation shall sever the data and give the individual access; (e) It would threaten the life, health or security of a person; (f) Data was collected under 4.3(b) (generally, collection pertaining to an investigation of a breach of an agreement or the law); (g) Complying with the request would be prohibitively costly to the organisation; or (h) The request is frivolous or vexatious.
6) Restrictions on onward transfers	**6) Restrictions on onward transfers** Further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the *Directive*.	**4.1.1** Where data are to be transferred to someone (other than the individual or the organisation or its employees), the organisation shall take reasonable steps to ensure that the data which is to be transferred will not be processed inconsistently with this Model Code.

WP12 Additional Principles

Working Party Principles		Model Data Protection Code
1) Sensitive data	**1) Sensitive data** Where 'sensitive' categories of data are involved (those listed in article 8 of the *Directive*), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.	**4.3 Principle 3—Consent** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal data to a third party, save where the following exceptions apply: […] **4.3.3** The form of the consent sought by the organisation may vary, depending upon the circumstances and the type of data. In determining the form of consent to use, organisations shall take into account the sensitivity of the data. **4.3.6** The way in which an organisation seeks consent may vary, depending on the circumstances and the type of data collected. An organisation should generally seek express consent when the data are likely to be considered sensitive. Implied consent would generally be appropriate when the data are less sensitive. **4.7 Principle 7—Safeguards** [see above] **4.7.2** The nature and extent of the safeguards will vary depending on: (a) the sensitivity of the data that have been collected; […]
	Article 8 **The processing of special categories of data** 1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the	

(*Continued*)

Working Party Principles		Model Data Protection Code
	processing of data concerning health or sex life. […] 5. Processing of data relating to offences, criminal convictions or security measures […] a complete register of criminal convictions may be kept only under the control of official authority. […] data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority. […] 7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.	
2) Direct marketing	**2) Direct marketing** Where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.	**4.3 Principle 3—Consent** [see above] Collection/use without knowledge or consent of the individual is permitted where: […] (h) Collection/use is of data which is generally available to the public. Disclosure without knowledge or consent of the individual is permitted where: […] (o) Disclosure is of data which is generally available to the public in that form.

(*Continued*)

(*Continued*)

Working Party Principles		Model Data Protection Code
		4.3.7 An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The individual may only be subjected to consequences because of this decision where the information is required to fulfil the specified, and legitimate purposes set out by the organisation (*e.g.* in the absence of the data on which to assess an individual's creditworthiness, an organisation may refuse to extend credit to him). The organisation should inform the individual of the implications of such withdrawal.
3) Automated individual decision	**3) Automated individual decision** Where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the *Directive*, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.	