COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 20.11.2006
SEC(2006) 1520

COMMISSION STAFF WORKING DOCUMENT

The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act

TABLE OF CONTENTS

1. INTRODUCTION

Directive 95/46/EC[1] (hereinafter "the Directive") provides for a special legal regime in cases of transfer of personal data to third countries. Article 25(1) stipulates that such transfers may only take place if the third country in question ensures an adequate level of protection. Article 25(6) empowers the Commission to issue decisions in this respect[2].

On 20 December 2001 the Commission issued Decision 2002/2/EC (hereinafter "the Decision") pursuant to Article 25(6) of the Directive stating that for the purposes of Article 25(2) of the Directive, Canada is considered as providing an adequate level of protection of personal data transferred from the Community to recipients subject to the Personal Information Protection and Electronic Documentation Act or PIPEDA (hereinafter 'the federal Canadian Act')[3].

Article 4(1) of the Decision stipulates that "the Commission shall evaluate the functioning of this Decision on the basis of available information, three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC[4], including any evidence that could affect the finding in Article 1 of this Decision that protection in Canada is adequate within the meaning of Article 25 of Directive 95/46/EC and any evidence that this Decision is being implemented in a discriminatory way."

This Working Document of the Commission services aims at presenting pertinent findings with regard to the functioning of the Decision as well as any findings with respect to any discriminatory implementation thereof. This paper does not aim at reviewing the content of the Decision itself. In order to acquire an accurate picture of the functioning of the Decision, a study was carried out for the Commission analysing the state of play in Canada as far as the application of the Decision is concerned (hereinafter "the study")[5]. The present paper is mainly based on this study.

2. METHODOLOGY

In order to assess transfers of personal data from the European Union to third countries, the group of Member States' national data protection supervisors, the so-called Article 29 Working Party (hereinafter "the Working Party"), formulated in its Working Paper 12[6] a number of core data protection principles and effective enforcement mechanisms compliance

---

1 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, OJ L 281, 23.11.1995, p. 31.

2 Commonly referred to as adequacy decisions.

3 OJ L 2, 4.1.2002, p.13.

4 Committee set up under Article 31 of the Directive and composed of the representatives of the Member States. This Committee must deliver an opinion before the Commission may adopt an adequacy finding.

5 Analysis of the Adequacy of Personal Data Protection in Canada (State of the situation 15 July 2005), CRID, Namur, July 2005 (hereafter referred to as the study).

6 Working Document of the Working Party entitled "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EC Data Protection Directive". DG XV D/5025/98.

with which would allow a determination that a third country's data protection system is adequate.[7]

The *core data protection principles* identified by the Working Party are the purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle, the rights of access, rectification and opposition and finally restrictions on onward transfers to other third countries. The Working Party also identified three additional issues to be looked into in cases of specific types of data processing, namely sensitive data, direct marketing and automated individual decisions. In terms of *enforcement requirements*, the Working Party identified three core elements: a good level of compliance, support and help to individual data subjects as well as appropriate redress.

The above-mentioned criteria have been used as evaluation criteria in order to assess the functioning of the Decision. The federal Canadian Act has been assessed also in the light of Opinion 2/2001 of the Working Party on the adequacy of the Act.[8] They have been further complemented by looking at the way the provisions of the Act have been interpreted and applied in practice since the Decision was taken.

3. ASSESSMENT OF CANADIAN COMPLIANCE WITH THE ADEQUACY DECISION

3.1. General findings

On the basis of the information received concerning the period under examination, the Commission services consider that the implementation of the Decision ensures the protection of individuals' privacy rights within the meaning of Article 25 of the Directive.

The Directive's principles are clearly reflected in the federal Canadian Act. Data transfers have to be limited to a specific purpose. Exceptions are those necessary in a free and democratic society (e.g.; national security, defence, public safety, criminal proceedings, protection of the data subject, scientific research). Data also have to be accurate, complete and up-to-date in view of the purpose for which they are collected and processed, thus reflecting the principles of data quality and proportionality. The federal Canadian Act further requires transparency (information to data subjects), access and correction rights and security measures aimed at protecting information. Onward data transfers are covered by the principle of responsibility, limiting transfers to recipients who are also subject to rules providing adequate protection. Additional protective measures are in place with respect to sensitive data, such as explicit consent.

The Commission services have not identified any major problems, either in terms of the implementation of the core data protection principles or in respect of the enforcement mechanisms in place in Canada. On the contrary, since the Decision entered into force, protection mechanisms and their implementation in Canada have been strengthened.

The federal Canadian Act, which would be implemented in three stages, came into full effect on 1 January 2004. This legislation now covers all information collected, used or disclosed by all private-sector organisations in the course of commercial activities, whether or not the organisation is a federally regulated business, or with respect to their employees in connection

---

[7] Idem.

[8] Document WP 39, 26 January 2001.

with a federal undertaking, except in provinces that have adopted legislation found to be substantially similar to the federal Canadian Act. Engagement in commercial activities is one of the main criteria to determine whether an organisation falls within the scope of the Act. This notion has been given a broad interpretation.

Provincial legislation on personal information is only declared substantially similar to the federal Canadian Act after thorough examination conducted in the light of criteria reflecting the Directive's principles. On the basis of a recommendation from the Minister of Industry, the Governor in Council will determine whether the legislation is substantially similar. If so, she will issue a decree, an Order-in-Council. The Privacy Commissioner is asked for her opinion, which forms part of the recommendation made to the Governor in Council. This process is intended to enable organisations operating only within one province to process data on the basis of one set of rules without jeopardizing the level of protection throughout Canada. As a result of this process, the laws of Québec[9], Alberta and British Columbia have been found similar to the federal Canadian Act through an Order-in-Council. This is of relevance in light of the Working Party's request to the Commission to examine this issue and assess whether provincial legislation had to be recognised individually as providing an adequate level of protection, or whether a determination that provincial legislation is substantially similar to the federal Canadian Act is sufficient to achieve the same purpose.

The Working Party also invited the Commission to follow the process with regard to health data. In this respect, health data are subject to protection flowing from a variety of laws, regulations and codes. These obligations are consistent with the federal Canadian Act and impose a duty to inform patients about the collection, use and dissemination of their health data, their consent in case of disclosure to third parties, access to personal medical files and proper disposal of medical information that is no longer necessary. The federal Canadian Act is applicable to all health care companies in private practice. However, the Act does not apply to hospital activities which are under provincial jurisdiction. In addition, the Act does not apply in provinces that have substantially similar privacy legislation in place. The British Columbia and Alberta acts have been declared substantially similar to the federal Canadian Act. The Ontario Personal Health Information Protection Act 2004 is in the process of being declared so. The legislation in force in Québec was already considered in line with the federal Canadian Act. Health care associations, in co-operation with the Privacy Commissioner, have issued guidance to help the sector to understand the scope and requirements of the federal legislation. [10]

In its Opinion the Working Party welcomed the systematic use of the highest level of protection when sensitive data are at stake. Although the federal Canadian Act does not make a distinction between different categories of data, particular attention is paid to the form of consent depending on the type of information. In determining the form of consent, organisations shall take into account the sensitivity of the information. Although medical records are almost always considered sensitive information, it is considered that any information can be sensitive, depending on the context. When information is considered sensitive, an organisation has to obtain explicit consent, the strongest form of consent. The

---

[9] However, Order-In-Council 1368-2003 makes a reference challenging the constitutional validity of the federal Canadian Act. The expected date for the hearing is now Spring 2007.

[10] Industry Canada, PIPEDA Awareness Raising Tools Initiative For The Health Sector, Questions and Answers, March 3, 2004, www.econ.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00235e.

Canadian Privacy Commissioner issued guidelines in this respect.[11] Sensitive data may also justify a restriction on an individual's right to access.

In some industries and business sectors, codes of conduct provide additional guarantees. Last but not least, the Canadian Charter of Rights and Freedoms provides major guarantees, although it does not contain specific provisions on privacy. The rights guaranteed by the Charter have the greatest protection. Legislation has to be consistent with the guarantees provided for by the Charter. The Charter applies to government activities, not to private organisations and companies.

Member States' data protection authorities have indicated that they did not experience difficulties in the context of data transfers to Canada in the framework of the federal Canadian Act during the period under examination.

Finally, Canadian legislation provides for appropriate institutional mechanisms, such as an independent supervisory authority with appropriate powers and appropriate recourse before the courts in case of violations of privacy. The Privacy Commissioner of Canada acts as an independent ombudsman and reports directly to the Parliament, not to the government in power. The Commissioner may investigate complaints and audit the way in which personal data are managed by organisations. The Commissioner cannot issue orders in cases of complaints, which prevents her from following up conclusions and recommendations made in her reports. However, after investigation of a complaint, complainants can appeal to the Federal Court.

3.2. Discrimination

In the Decision the Commission is also requested to look into the issue of possible discriminative implementation of the Decision. Neither the study, nor other information collected by the Commission services has revealed any case of discriminatory implementation.

4. CONCLUSION

On the basis of the study and other information collected, the Commission services take the view that the Canadian Personal Information and Electronic Documentation Act continues to provide an adequate level of protection of personal data within the meaning of Article 25 of the Directive.

The reservation formulated in Article 3 of Decision 2002/2/EC[12] which contains safeguards necessary in case of data transfers to countries outside the European Union is maintained.

---

[11] Fact sheet, 28 September 2004, www.privcom.ga.ca/fs-fi.

[12] Article 3 of the Decision allows the national data protection authorities of the EU Member States to suspend data flows to a recipient in Canada in a number of specified cases listed in this article.