EUROPEAN COMMISSION
Internal Market DG

Functioning and impact of the Internal Market. General affairs and coordination.

Brussels,
MARKT/E1//FB/fb D(2000)

Submission

to the
House of Representatives Committee on Legal and Constitutional Affairs concerning its inquiry into the

Privacy Amendment (Private Sector) Bill 2000

Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgium - Office: C107 2/29.
Telephone: direct line (+32-2)2963285, switchboard 299.11.11. Fax: 2994745.
Telex: COMEU B 21877. Telegraphic address: COMEUR Brussels.

Summary

The services of the European Commission are grateful for the opportunity to express their views on the Privacy Amendment (Private Sector) Bill, especially with regard to some of the issues that need to be examined before an "adequacy" finding by the European Commission can be made.

Our interest stems from the implementation of the EU's Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Directive harmonises Member States' data protection laws with a view to ensuring the free movement of personal data within the EU while ensuring that the privacy of individuals enjoys a high level of protection.

The Directive also establishes rules designed to ensure that data is only transferred to non-EU countries when its continued adequate level of protection is guaranteed. Without such rules, which are in full compliance with the GATS agreement, the high standards of data protection established by the Directive would quickly be undermined. One means by which such "adequacy" can be determined is through a decision by the Commission based on a country's domestic law.

We note that one of the objectives of the legislation, as stated in the Explanatory Memorandum to the Bill, is for a scheme which is "compatible with the European Union Directive…to remove potential barriers to trade".

The comments below concern exclusively the Privacy Amendment (Private Sector) Bill to the extent it applies to private sector organisations. We have a range of issues which we would like to raise: some are principally to gain clarification on how the Bill is intended to operate; while others note our concern that, as currently drafted, the Bill may not provide an adequate level of protection for European citizens.

Scope: The exclusion of employee data and small business will mean that these sectors cannot be included in any consideration of "adequacy" being provided by the Bill. In particular, we envisage the exclusion of small businesses would be problematical, since it would be very difficult in practice to identity small business operators before exporting the data to Australia.

The exception for generally available publication: We are keen to understand to what extent you have chosen to exempt generally available publications from the protection of the Bill, as too broad an exemption could undermine the protection afforded by the Bill.

Data export regime: We are keen to have more detailed information on how NPP9 (a) will operate in practice. One solution to minimise the uncertainty would be for the Privacy Commissioner to indicate what third country regimes can be considered as substantially similar to your domestic situation.

We are also keen to obtain more detailed information on how NPP 9(f) will work. If our reading is correct, it seems to offer less rights. Notably the individuals' right to see his rights enforced and that no compulsory recourse for the individual is guaranteed.

But our most important concern on this point regards the protection awarded to European citizens when their data is exported from Australia. In this respect, Section 5 on the extra territorial operation of the Act, applies only to Australians and *does not extend the protection of NPP9 to non-Australians.*

Lack of correction rights for EU citizens: A similar situation of great concern is the exercise of access and correction rights under NPP 6 and 7. As currently drafted the Bill excludes *non-Australians*.

Data sharing between body corporates and partnership: We are concerned that the individual is not able to opt-out of such data sharing. Our concern is heightened by the fact that small business operators are exempt from the obligations of the protection of the Bill.

Exceptions to substantive data protection principles on the grounds that it is authorised by law. We are concerned at the broad scope of the exception under NPP 2.1(g), which risks undermining legal certainty and devaluing the content of the basic protection.

Transparency to data subjects: Our concern under Principle 1.3 is that it provides an exception to the requirement to inform individuals as to purposes of collection before or at the time of collection of the information.

Complaints dealt by industry bodies: With reference to s18BB(3) and s18BB(k), we would appreciate clarification as to requirements that industry enforcement bodies have to respect. In particular if decisions of such bodies are made public and if they have to be duly motivated?

Introduction

The services of the European Commission are grateful for the opportunity to express their views on the Privacy Amendment (Private Sector) Bill to the Legal and Constitutional Affairs, especially with regard to some of the issues that need to be examined before an "adequacy" finding by the European Commission can be made. We are also grateful for the exchanges of information and views that have taken place on several occasions with the Attorney General's Department.

We note that in the Explanatory Memorandum to the Bill it states, amongst other objectives, the Government aims to ensure that any scheme:

> "is compatible with the *European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* to remove any potential barriers to international trade."

We also note that the Hon. Mr Williams, the Attorney-General, in the Bill's second reading speech stated:

> "I am confident that this bill will provide adequate privacy safeguards to facilitate future trade with EU members"

It is in the light of these statements, and a desire to contribute constructively at an early stage to the debate on what meets the "adequacy" requirements before any formal process commences, that this submission is made.

Before doing so, we would like to take this opportunity to sketch the general outline of the EU Data Protection Directive and its implementation to date as well as the conditions under which the Commission is able to find that a third country provides for an adequate level of protection for the transfer of personal data from the EU.

The protection of personal data in the EU

In the EU, the protection of personal data in ensured by Directive 95/46 of 24th October 1995[1]. The Directive harmonises Member States' data protection laws with a view to ensuring the free movement of personal data within the EU while ensuring that the privacy of individuals enjoys a high level of protection. The *raison d'être* of the Directive is thus the Single Market. Without the Directive, different national approaches to data protection would create barriers within the market and the free movement of personal information would be impaired.

The Directive is a framework instrument, establishing basic principles, which are applicable to all types of personally identifiable data, by whatever means they are processed. It places obligations on those who collect, process or transfers personal data and accords rights to data subjects. As of today, nine Member States have implemented its provisions into national law. The European Commission has initiated proceedings before the Court of Justice against the remaining Member States for failure to comply with the obligation to transpose its requirements into their national legislation by 25th October 1998.

---

[1] Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data in Official Journal L281 of 23 November 1995, p.31

The Directive also establishes rules designed to ensure that data is only transferred to third countries when its continued protection is guaranteed or when certain specific exemptions apply (Articles 25 and 26). Without such rules, which are in full compliance with the GATS agreement, the high standards of data protection established by the Directive would quickly be undermined, given the ease with which data can be moved around on international networks. The Directive provides for the blocking of specific transfers where necessary, but this is a solution of last resort and there are several other ways, namely through Article 26, of ensuring that data continues to be adequately protected while not causing disruption to international data flows and the commercial transactions with which they are associated.

In implementing the Directive, the Commission is assisted by a committee and a working group. The committee, set up by Article 31 of the Directive, is composed of Member State officials. Its particular task is to advise the Commission concerning decisions on the adequacy of the protection of individuals with regard to the processing of personal data for the purpose of transferring it to third countries. The working group, set up by Article 29, is composed of the data protection commissioners or independent supervisory authorities of all the Member States. Its remit is wider than that of the committee and it will in particular play an important role in helping the Commission to ensure the even application of the Directive's requirements across the EU. The Article 29 group is also asked to advise on certain aspects of data transfers to third countries.

The Council and the European Parliament have given the Commission the power to determine, on the basis of Article 25.6, whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. Following the advice of the group of the data protection commissioners, the Commission has recognised that an adequate level of protection could also be provided by sector specific legislative act or effective self-regulatory scheme, for example one whose enforcement was underpinned by law[2].

The adoption of a (comitology) Commission decision based on Article 25.6 of the Directive involves a proposal from the Commission, an opinion of the group of the national data protection commissioners (non-binding) and an opinion of the Article 31 Management committee delivered by a qualified majority of Member States. The European Parliament has a thirty-day period within which to exercise its right of scrutiny to check if the Commission has used correctly its executing powers, before the Commission adopts its decision. The formal process of considering whether a specific legislative act meets the "adequacy" requirement can only commence once the relevant legislation is passed.

The effect of such a decision is that data can flow to that third country without any further safeguard being necessary. The Commission has so far proposed to recognise Switzerland, Hungary and the US Department of Commerce's Safe harbor as providing adequate protection. These proposals have been considered by the Member States and once the European Parliament has delivered its opinion, scheduled for the month of July, the European Commission will be able to adopt its proposed decisions.

Privacy Amendment (Private Sector) Bill 2000

---

[2] WP12: Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive, adopted by the Working Party on 24 July 1998

The comments below concern exclusively the Privacy Amendment (Private Sector) Bill to the extent it applies to private sector organisations and does not include considerations relating to public sector bodies or on the level of adequacy provided by the Public Sector Act.

Scope: We take note that the Bill does not cover employee data and small business. This is a choice that we fully respect. However, we would like to draw your attention to the fact that in the event of the Bill being recognised as providing adequate protection by the EU these sectors would be excluded from the decision. Whereas it would be straightforward to exclude employee data from its scope (in which case the provisions of the Directive would have to be respected by putting into place standard contract clauses for the transfer of such data, Article 26.4); it would be very difficult in practice to identity small business operators, before exporting the data to Australia. Moreover, it is not clear if small business wishing to import data from the EU can voluntarily adhere to the provisions of the Act or what other means are at their disposal to provide an adequate level of protection.

The exception for generally available publication: You are undoubtedly aware that neither the EU Directive nor the 1980 OECD guidelines refer to or contain an exemption for publicly available data. In the Directive, the only reference to a similar, stricter provision is to be found in Article 26 paragraph 1 (f). This provision allows personal data transfers from a EU public register to a third country which does not provide adequate protection, only to the extent that the conditions laid down in law for the consultation of the register are respected. The reason for this limitation is simple – if not monitored, publicly available information can easily be misused for new purposes not covered by the original publication and used to build extremely detailed personal profiles. A simple example may suffice – reverse searching of property registers allows to identify very quickly an individual's property holdings. These and other similar practises relating to publicly available data, which are not in public registers, have already been declared unlawful in some EU Member States. Another issue to be considered is whether individuals are able to opt-out of registers that are rendered available to the public. For example, one Member State (the United Kingdom) is in the process of changing its law on the electoral register to ensure that citizens have a right to opt out of the electoral roll.

We are keen to understand to what extent you have chosen to exempt generally available publications (i.e. magazine, book, newspaper or other publication that is or will be generally available to members of the public, however published - S6, schedule 1, item 14) from the protection of the Bill and this irrespective of whether or not there has been circumvention of the protection it offers. On the basis of the above, we would caution you to deny information and access rights to individuals with regard to publicly available data and we find this provision to be potentially a great hole in the comprehensive protection provided by the Bill.

Data export regime: NPP 9 prohibits exports of personal information by an organisation to someone in a foreign country (other than an affiliate of the organisation itself) unless one of six conditions applies. This is broadly similar to what is applicable under the EU Directive. This said, we would like to draw your attention to the following three points:

> "NPP9 (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles.

We are keen to have more detailed information on how this provision will operate in practice. It is our experience that it is difficult for the average operator to have a substantial knowledge of the level of protection of personal data in third countries. Exonerating an operator of all responsibility under the Act simply by applying a reasonable belief test is likely to create uneven conditions for data transfers outside Australia. Also the existence of a law, a contract or a binding scheme is in itself an objective fact that can be ascertained, hence the reasonably belief test is somewhat unsettling. We believe that in this instance, the assistance of the Privacy Commissioner in indicating what third country regime can be considered as substantially similar to your domestic situation is advisable.

> ”NPP 9(f), the organisations has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles”.

Again we are keen to obtain more detailed information on how this provision will work. If our reading is correct, it will used when (a) will not apply, that is when the recipient is not subject to a law, binding scheme or contract. In this case, it is sufficient for the transferor to reasonably ensure that the information is not held, used or disclosed by the recipient. This provision however does not take into account the individuals’ right to see his rights enforced and no compulsory recourse for the individual is guaranteed. In fact, it seems to offer less.

But our most important concern on this point regards the protection awarded to European citizens when their data is exported from Australia. In this respect, Section 5 on the extra territorial operation of the Act, applies only to Australians and *does not extend the protection of NPP9 to non-Australians.* This means that an Australian company can import data from European citizens and subsequently export it to a country with no privacy laws without the Australian Act applying. Such a measure would make it possible to circumvent the EU Directive, if Australia was recognised as providing adequate protection.

Lack of correction rights for EU citizens: A similar situation of great concern is the exercise of access and correction rights under NPP 6 and 7. Section 41 (4) allows the Privacy Commissioner to investigate an act or practice under NPP 6 or 7 only if it is an interference with the privacy of Australian citizens and the permanent residents. Thus this limitation specifically excludes EU citizens. We would very much appreciate if consideration could be given to extending the Privacy Commissioner’s ability to intervene when the act and practice concerns correction rights of any individual without any reference to the nationality of the individual.

Data sharing between body corporates and partnership: Disclosure to, or collection from a related body corporate or related partnership will not breach any principles unless

the information is sensitive. We would be grateful for further information on the practical application of this exception. Our understanding from the Explanatory Memorandum is that each body corporate within the group must nonetheless use the information consistently with the main purpose for which it was originally collected and may only use the information for a secondary purpose where the purpose is allowed by NPP 2.1. Although we also note that the body corporate must provide the individual with information as to the parties with whom it shares the data, we remain concerned that the individual is not able to opt-out of such data sharing. Our concern is heightened by the fact that small business operators are exempt from the obligations of the protection of the Bill.

Exceptions to substantive data protection principles on the grounds that it is authorised by law. National Privacy Principle NPP 2.1 (g) allows information to be used or disclosed for a secondary purpose where the use or disclosure is required or authorised by law. According to the Explanatory Memorandum, the reference to "authorised" encompasses circumstances where the law permits, but does not require, use or disclosure.

In our view, it is perfectly acceptable to provide for an exception when organisations are faced with conflicting legal obligations, but to widen the exception to cover all options offered by sector specific laws, past present and future, risks undermining legal certainty and devaluing the content of the basic protection. We are aware that NPP 1.3 (e) requires the organisation to inform the individual of any law that requires a particular information to be collected. We remain very keen however, to understand the extent of the exception, namely: a) specific examples of when use and disclosure is simply carried out on the basis of an authorisation; and b) confirmation of the extent to which the individual can object to the use and disclosure.

Transparency to data subjects: Principle 1.3 allows for organisations to inform individuals before or at the time of collection but also adds that, if this is not practicable, it may inform individuals as soon as practicable thereafter. We note from the Explanatory Memorandum that where the information is collected via the Internet, NPP 1.3 would require that a policy statement appear on the web page notifying the individual of contact details of the organisation collecting the information and outlining in what circumstances, and for what purposes personal information (such as email address, name or other personal details including purchasing habits linked to an email address) is collected. Our concern here is to encourage the provision of *specific* information as to purposes of collection to the individual not later than at the time of collection.

Complaints dealt by industry bodies: With reference to s18BB(3) and s18BB(k), we would appreciate to have clarification as to requirements that industry enforcement bodies have to respect. In particular, if decisions of such bodies are made public and if they have to be duly motivated? Our interest here lies with the requirements of the enforcement of self-regulation when they have to fulfil comparable characteristics that are otherwise covered by a public enforcement system.

Once again we are grateful for this opportunity to express our views and remain at the disposal of the Committee and of the Attorney General's office for any further clarifications.