EUROPEAN COMMISSION
DIRECTORATE GENERAL XV
Internal Market and Financial Services
Free movement of information, company law and financial information
Free movement of information and data protection, including international aspects

DG XV D/5057/97 final
WP 7

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

Working Document: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?

Adopted by the Working Party on 14 January 1998

WORKING DOCUMENT

JUDGING INDUSTRY SELF-REGULATION: WHEN DOES IT MAKE A MEANINGFUL CONTRIBUTION TO THE LEVEL OF DATA PROTECTION IN A THIRD COUNTRY?

Introduction

Article 25(2) of the data protection directive (95/46/EC) requires the level of protection afforded by a third country to be assessed in the light of *all the circumstances* surrounding a data transfer operation or set of such operations. Specific reference is made not only to rules of law but also to "professional rules and security measures which are complied with in that country."

The text of the directive therefore requires that account be taken of non-legal rules that may be in force in the third country in question, provided that these rules *are complied with.* It is in this context that the role of industry self-regulation must be considered.

What is self-regulation?

The term "self-regulation" can mean different things to different people. For the purpose of this document, self-regulatory code (or other instrument) should be taken to mean any set of data protection rules applying to a plurality of data controllers from the same profession or industry sector, the content of which has been determined primarily by members of the industry or profession concerned.

This is a broad definition which would encompass, at one end of the scale, a voluntary data protection code developed by a small industry association with only a few members, to at the other end, the kind of detailed codes of professional ethics applicable to entire professions, such as doctors and bankers, which often have quasi-judicial force.

Is the body responsible for the code representative of the sector?

As this document will go on to argue, one important criterion for judging the value of a code is the degree to which its rules can be enforced. In this context, the question of whether the association or body responsible for the code represents all the operators in a sector or only a small percentage of them, is probably less important than the strength of the association in terms of its ability to, for example, impose sanctions on its members for non-compliance with the code. However, there are several secondary reasons which render industry-wide or profession-wide codes with clearly comprehensive coverage more useful instruments of protection than those developed by small groupings of companies within sectors. First is the fact that, from the consumer's point of view, an industry that is fragmented and characterised by several rival associations, each with its own data protection code, is confusing. The co-existence of several different codes creates an overall picture which lacks transparency for the data subject. The second point is that, particularly in industries such as direct marketing, where personal data is routinely passed between different companies of the

same sector, situations can arise where the company disclosing personal data is not subject to the same data protection code as the company that receives it. This is a source of considerable ambiguity as to the nature of the rules applicable, and it might also render investigation and resolution of complaints from individual data subjects extremely difficult.

Evaluating self-regulation - the approach to take

Given the wide variety of instruments which fall within the notion of self-regulation, it is clear that there is a need to differentiate between the various forms of self-regulation in terms of their real impact on the level of data protection applicable when personal data are transferred to a third country.

The starting point for the evaluation of any specific set of data protection rules (whether categorised as self-regulation or regulation) must be the general approach set down in the discussion document "First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy". The cornerstone of this approach is an examination not only of the content of the instrument (it should contain a series of core principles) but also of its effectiveness in achieving:

- a good level of general compliance
- support and help to individual data subjects
- appropriate redress (including compensation where appropriate).

Evaluating the content of a self-regulatory instrument

This is a relatively easy task. It is a question of ensuring that the necessary 'content principles' set out in the "First Orientations" document are present (see extract attached). This is an objective evaluation. It is a question of what the code contains, and not how it was developed. The fact that an industry or profession has itself played the major role in developing the content of the code is not in itself relevant, although clearly if the opinions of data subjects and consumer organisations have been taken into account during its development, it is more likely that the code will reflect more closely the core data protection principles which are required.
The transparency of the code is a crucial element; in particular, the code should be drafted in plain language and offer concrete examples, which illustrate its provisions.
Furthermore, the code should prohibit the disclosure of data to non-member companies who are not governed by the code, unless other adequate safeguards are provided.

Evaluating the effectiveness of a self-regulatory instrument

Assessing the effectiveness of a particular self-regulatory code or instrument is a more difficult exercise, which requires an understanding of the ways and means by which adherence to the code is ensured and problems of non-compliance dealt with. The three functional criteria for judging the effectiveness of protection must all be met if a self-regulatory code is to be taken into consideration in the assessment of adequacy of protection.

Good level of compliance

An industry or professional code will typically be developed by a representative body of the industry or profession concerned, and it will then apply to members of that particular representative body. The level of compliance with the code is likely to depend on the degree of awareness of the code's existence and of its content among members, on the steps taken to ensure transparency of the code to consumers in order to allow the market forces to make an effective contribution, on the existence of a system of external verification (such as a requirement for an audit of compliance at regular intervals) and, perhaps most crucially, on the nature and enforcement of the sanction in cases of non-compliance

Important questions are therefore:

- what efforts does the representative body make to ensure that its members are aware of the code?
- does the representative body require evidence from its members that it has put the provisions of the code into practice? How often?
- is such evidence provided by the member company itself or does it come from an external source (such as an accredited auditor)?
- does the representative body investigate alleged or suspected breaches of the code?
- is compliance with the code a condition of membership of the representative body or is compliance purely "voluntary"?
- where a member has been shown to breach the code, what forms of disciplinary sanction are available to the representative body (expulsion or other) ?
- is it possible for an individual or company to continue working in the particular profession or industry, even after expulsion from the representative body?
- is compliance with the code enforceable in other ways, for example by way of the courts or a specialist tribunal? Professional codes of ethics have legal force in some countries. It might also be possible in some circumstances to use general laws relating to fair trading practice or even competition to enforce industry codes.

When examining the types of sanction in place, it is important to distinguish between a "remedial" sanction which simply requires a data controller, in a case of non-compliance, to change its practices so as to bring them into line with the code, and a sanction which goes further by actually punishing the controller for its failure to comply. It is only this second category of "punitive" sanction which actually has an effect on the future behaviour of data controllers by providing some incentive to comply with the code on an ongoing basis.

The absence of genuinely dissuasive and punitive sanctions is therefore a major weakness in a code. Without such sanctions it is difficult to see how a good level of overall compliance could be achieved, unless a rigorous system of external verification (such as a public or private authority competent to intervene in case of non compliance with the code, or a compulsory requirement for external audit at regular intervals) were put in place.

Support and help to individual data subjects

A key requirement of an adequate and effective data protection system is that an individual faced with a problem regarding his/her personal data is not left alone, but is given some institutional support allowing his/her difficulties to be addressed. This institutional support should ideally be impartial, independent and equipped with the necessary powers to investigate any complaint from a data subject. Relevant questions for self-regulation in this regard are:

- is there a system in place allowing for investigation of complaints from individual data subjects?
- how are data subjects made aware of this system and of the decisions taken in individual cases?
- are there any costs involved for the data subject?
- who carries out the investigation? Do they have the necessary powers?
- who adjudicates on an alleged breach of the code? Are they independent and impartial?

The impartiality of the arbiter or adjudicator in any alleged breach of a code is a key point. Clearly such a person or body must be independent in relation to the data controller. However, this in itself is not sufficient to ensure impartiality. Ideally the arbiter should also come from outside the profession or sector concerned, the reason being that fellow members of a profession or sector have a clear commonality of interests with the data controller alleged to have breached the code. Failing this the neutrality of the adjudicating body could be ensured by including consumer representatives (in equal numbers) alongside the industry representatives.

Appropriate Redress

If the self-regulatory code is shown to have been breached, a remedy should be available to the data subject. This remedy must put right the problem (e.g. correct or delete any inaccurate data, ensure that processing for incompatible purposes ceases) and, if damage to the data subject has resulted, allow for the payment of appropriate compensation. It should be borne in mind that "damage" in the sense of the data protection directive includes not only physical damage and financial loss, but also any psychological or moral harm caused (known as "distress" under UK and US law).

Many of the questions regarding sanctions listed above in the section "Good level of compliance" are relevant here. As explained earlier sanctions have a dual function: to punish the offender (and thus encourage compliance with the rules by the offender and by others), and to remedy a breach of the rules. Here we are primarily concerned with the second of these functions. Additional questions would therefore include:

- is it possible to verify that a member who has been shown to contravene the code has changed his practices and put the problem right?
- can individuals obtain compensation under the code, and how?
- is the breach of the code equivalent to a breach of contract, or enforceable under public law (e.g. consumer protection, unfair competition), and can the competent jurisdiction award damages on this basis?

Conclusions

- Self-regulation should be evaluated using the objective and functional approach set out in the "First Orientations" document.
- For a self-regulatory instrument to be considered as a valid ingredient of "adequate protection" it must be binding on all the members to whom personal data are transferred and provide with adequate safeguards if data are passed on to non-members.
- The instrument must be transparent and include the basic content of core data protection principles.
- The instrument must have mechanisms which effectively ensure a good level of general compliance. A system of dissuasive and punitive sanctions is one way of achieving this. Mandatory external audits are another.
- The instrument must provide support and help to individual data subjects who are faced with a problem involving the processing of their personal data. An easily accessible, impartial and independent body to hear complaints from data subjects and adjudicate on breaches of the code must therefore be in place.
- The instrument must guarantee appropriate redress in cases of non-compliance. A data subject must be able to obtain a remedy for his/her problem and compensation as appropriate.

EUROPEAN COMMISSION
DIRECTORATE GENERAL XV
Internal Market and Financial Services
Free movement of information, company law and financial information
Free movement of information and data protection, including international aspects

XV D/5020/97-EN final
WP4

ANNEX

WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy

Discussion Document adopted by the Working Party on 26 June 1997

(i) Content Principles

It is suggested that the basic principles to be included are the following:

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.

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.

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 the Articles 11(2) and 13 of the directive.

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.

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.

6) restrictions on onward transfers to other third countries - further transfers of the personal data from the destination third country to another third country should be permitted only where the second third country also affords an adequate level of protection. The only exceptions permitted should be in line with Article 26 of the directive

Examples of additional principles to be applied to specific types of processing are:

1) **sensitive data** - where 'sensitive' categories of data are involved (those listed in article 8), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

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.

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.