ARTICLE 29 - DATA PROTECTION WORKING PARTY

11639/02/EN
WP 74

Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers

Adopted on 3 June 2003

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

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

has adopted the present Working Document:

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

INDEX

page

Working Document on Binding Corporate Rules for International Data Transfers

1. INTRODUCTION

Data Protection Authorities receive requests for authorisations for the transfer of personal data to third countries within the meaning of Article 26 (2) of the Directive. Traditionally most of these requests have required contractual solutions which national authorities have considered in the light of the principles outlined in WP 12[2], other documents issued by this group and particularly the Commission decisions on standard contractual clauses.

Contractual solutions have been already used by multinational companies and the possibility of broadening their use is now under discussion in some Member States. These experiences must be taken into account seriously for evaluating the possible developments of the regulation in these matters.

At the same time, some multinational companies due to their complex architectural structures worldwide would like to benefit from the possibility to adopt "codes of conduct for international transfers"[3] dealing with the international transfer of personal data within the same corporate group at a multinational level subject to the authorisation of the relevant data protection authorities, under Art. 26 (2) of the Directive,. These multinational companies are also of the view that the possibility of unilateral undertakings surrounded by solid guarantees should also be exploited.

In so far as a unilateral undertaking is able to deploy real and ensured legal effects, in particular as regards the effective protection of data subjects after the transfer and as regards the possible intervention of national supervisory authorities or other authorities, as further clarified under chapters 3 and 5 below, there should not be any reason to exclude such a possibility: Article 26 (2) of Directive 95/46/EC offers the Member States a broad margin of manoeuvre in this regard.

However, it is important to recognise that under the national law of some Member States, unilateral undertakings do not create obligations and rights with legal effects. In

---

2 Working document: Transfer of personal data to third countries: applying Articles 25 and 26 of the EU Data Protection Directive, approved on 24 July 1998.

4 The adoption of codes of conduct by corporate groups is relatively frequent. Typical subjects of codes of conduct adopted by multinationals would be the following: (a) maintenance and retention of accurate books and records; (b) truthfulness and accuracy in communications with the public and the government; (c) procedures such as Chinese walls to assure that advice to clients and business decisions are not affected by conflicts of interest; (d) protection of confidential information; (e) prohibition of misuse of corporate assets; (f) elimination of improper discrimination and harassment; (g) prohibition of bribery and kickbacks; (h) implementation of ethical business practices and compliance with laws that foster competition in the marketplace; and (i) prohibition of securities trading based on inside information

consideration of that, the Working Party intends to stress the general nature of the present document on the subject matter in order to avoid the risk to interfere with the applicable national legislations and reserves the right to provide further solutions that may harmonise further the use of binding corporate rules in all Member States.

Binding corporate rules should not be considered as the only or the best tool but for carrying out international transfers but only as an additional one where the use of existing instruments (i.e. Commission decisions on standard contractual clauses or the Safe Harbor Principles where applicable) seem to be particularly problematic. This working document may not be used as forcing or even simply as inciting the Member States to use a given tool in responding to the requests of multinational companies. National supervisory authorities or any other competent bodies are entirely free to analyse and answer the proposals submitted to them in the way that fits best with their national laws and the given elements of the submission

The Working Party is of the view nevertheless that it is useful to extend these reflections to the Community level and agree on a series of principles and procedures which will both facilitate the work for companies and authorities in the Member States and guarantee consistency within the EU. In any case this working document aims at contributing to a more harmonised application and interpretation of Article 26 (2) of the Directive in the Member States and facilitating data flows in cases where adequate protection is provided. [4]

Finally, the Article 29 Working Party would like to reiterate that adducing sufficient safeguards within the meaning of Article 26 (2) is a broad concept that certainly includes contractual solutions and binding corporate rules but may also cover other situations not dealt with by this paper which data protection authorities can also consider suitable for the granting of authorisations. This working document, nevertheless, has reviewed the application of Article 26 (2) of the Directive in the particular case of the binding corporate rules.

The Article 29 Working Party also shares the concern expressed by some national data protection authorities in the sense that they may lack sufficient resources to deal with numerous requests for authorisations in a lengthy and negotiable manner. It is confident that corporations will bear these limitations in mind and will endeavour to submit applications as close as possible to the recommendations contained in this working document.

2. THE POTENTIALITIES OF CONTRACTUAL SOLUTIONS

The Article 29 Working Party would like to stress that the fact that this working document focus on binding corporate rules (or codes of conduct in more traditional terminology) should not be interpreted as indicating that contractual solutions have been superseded. On the contrary, after the Commission decisions on standard contractual clauses and the considerable guidance provided by this Working Party and national data protection authorities, companies are making broad use of these instruments in a very

positive and encouraging way (e.g. the standard contractual clauses with many parties to the contract).

The Article 29 Working Party believes that the potential of standard contractual clauses has only begun being exploited by operators. Two issues must be pointed out in this regard.

First, the Commission decisions on standard contractual clauses prevent a Member State from determining that a data exporter ready to enter into a contract in line with the standard contractual clauses does not offer sufficient safeguards for the transfer to take place, except in the particular circumstances specified by the Commission decisions. In other words, the standard contractual clauses are a useful, practical tool – at the moment already available for operators – legally recognised and adopted at both EU and national level, which provides an equal, sufficient level of harmonised guarantees for operators and data subjects. At the same time, Member States are entitled to consider other contractual arrangements as long as they undoubtedly assure a sufficient level of protection for the personal data concerned.

Secondly, it seems also possible, on the basis of the use of standard contractual clauses, to envisage the use of the binding corporate rules to allow, under certain conditions[5], onward transfers to other recipients different from the data importer without other contracts being necessary with these further recipients. There appears to be an interesting combination to consider between the contractual solutions and the use of the binding corporate rules that may overcome the obstacles posed by the lack of legal effects of unilateral undertakings in some Member States. Thus, the circulation of personal data within the members of the corporate group might be allowed under this solution, provided the necessary guarantees are put into place.

3. DEFINITION AND LEGAL ISSUES AT STAKE

3.1. Scope of this instrument and definitions

When dealing with requests under Article 26 (2) of the Directive, the assessment for granting an authorisation consists of an analysis of the safeguards put in place by the controller in order to guarantee an adequate protection of the personal data with regard to its transfer to a third country.

This exercise is therefore different from the approval of codes of conduct provided for in Article 27 of the Directive, that is, professional rules aimed at the practical application of national data protection legislation in a specific sector. In either case, the internal rules of a corporate group cannot replace the data protection obligations by which the members of the corporate group are bound by law. Compliance with national law is of course a condition *sine qua non* for any authorisation to be granted.

[5] For example by identifying in the contract the further recipients and attaching the binding corporate rules as an annex to the contract, but at the same time as an integral part of it, with all legal consequences.

A transfer to a third country consists of the communication of data to another data controller or data processor in a third country, the legitimacy of which should be assessed by reference to the general circumstances of the case with regards to the principles set up by the Directive (Articles 6, 7, 8, 17, etc.). Where the processing is carried out in the context of the activities of an establishment of a member of a corporate group on Community territory or the processing is carried out by a member of the corporate group who is not established on Community territory but makes use of equipment situated on Community territory, the Directive and national laws of implementation apply.

The principles of protection contained in the binding corporate rules must comply to a large extent with the principles of protection of Directive 95/46/EC. From this perspective, as a general principle, the implementation of binding corporate rules within the Community does not pose any problem provided that the rules comply with the national data protection legislation. If these conditions were met, this would allow corporate groups to have a truly global privacy policy.

In the same line of thought and by definition, binding corporate rules are global and therefore no distinction should be made in their application. The rules must apply generally throughout the corporate group irrespective of the place of establishment of the members or the nationality of the data subjects whose personal data is being processed or any other criteria or consideration. However, whilst the rules would always remain the same and the corporate group would endeavour to respect them accordingly, their enforceability vis-à-vis the corporate group may legitimately differentiate between data originating in the EU, in other words, personal data that were once subject to EU law and subsequently transferred abroad, and other categories of data.

For this latter category of data, the corporate group is not obliged to entitle data subjects to claim or enforce any rights on Community territory. Although such an inclusion cannot be regarded as a *condition sine qua non* for the granting of an authorisation, it would always be very welcomed and regarded as a serious commitment of the corporate group to data protection requirements.

Consequently, as the purpose of these instruments is different from the codes of conduct foreseen in Article 27 of the Directive, rather than referring to them as "codes of conduct" (which could be misunderstood) it seems more appropriate to find a terminology which fits with the real nature of these instruments, that is, the provision of sufficient safeguards for the protection of personal data transferred outside the Community.

A possible terminology for these instruments could be **"binding corporate rules for international data transfers" or "legally enforceable corporate rules for international data transfers"**

a) **binding or legally enforceable** because only with such a character may any clauses be regarded as "sufficient safeguards" within the meaning of Article 26 (2)

b) **corporate** in the sense that they consist of the rules in place in multinational companies, usually set up under the responsibility of the headquarters. For the purposes of this document, a corporate group is any group of companies which are effectively bound by the rules as provided for in chapter 3.3.

c) **for international data transfers** as the main reason for their existence.

The notion of "corporate group" may vary from one country to another and may correspond to very different business realities: from closely-knit, highly hierarchically structured multinational companies to groups of loose conglomerates; from groups of companies sharing very similar economical activities and therefore processing operations to broad partnerships of companies with very different economical activities and different processing operations. Obviously, these differences in structure and activity impacts upon the applicability, design and scope of the binding corporate rules and corporate groups must bear this in mind when submitting their proposals.

For loose conglomerates, binding corporate rules are very unlikely to be a suitable tool. The diversity between their members and the broad scope of the processing activities involved would make it very difficult (if not impossible) to meet the requirements outlined in this working document. For these conglomerates it would be necessary to differentiate subgroups within the same corporate group, set up severe limitations and conditions for the exchanges of information and particularise the rules. In other words, should a final product end up being acceptable under Article 26 (2) of the Directive, it would certainly look like very different from the binding corporate rules discussed in this working document.

In practice, it is expected that multinational companies will be the most frequent users of these mechanisms, as they will want to regulate intra-group transfers world-wide in this way. The Article 29 Working Party would like to stress again the fact that the scope of any authorisation granted on the basis of this instrument would only concern transfers or categories of transfers within the corporate group, in other words, exchanges of personal data between companies bound by these corporate rules. Transfers of personal data to companies outside the corporate group would remain possible but not on the basis of the arrangements put in place by legally enforceable corporate rules but on the basis of any other legitimate grounds under Article 26 of the Directive (e.g. under standard contractual clauses- model contracts or ad hoc ones- concluded with the recipients of the information).

3.2. Onward transfers

Onward transfers, that is, transfers from members of the corporate group outside of the Community to companies outside the corporate group would be possible by subscribing the standard contractual clauses adopted by the European Commission in its decision 2001/497/EC (transfers to data controllers) and 2002/16/EC (transfers to data processors) or on the conditions set up therein.

In accordance with this decision, further transfers of personal data to another controller established in a third country not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25 (6) of the Directive may take place if the data subjects have, in the case of special categories of data, given their unambiguous consent to the onward transfer, or, in other cases, have been given the opportunity to object.

The minimum information to be provided to data subjects should contain, in a language understandable to them:

- the purposes of the onward transfer
- the identification of the data exporter established in the Community from where the personal data originates

- the categories of the further recipients of the personal data and the countries of destination

- an explanation that, after the onward transfer, data may be processed by a controller who is not bound by the binding corporate rules and is established in a country where there is not an adequate level of protection of the privacy of individuals.

The regular audits foreseen in Chapter 4.4. of the binding corporate rules should contain a specific chapter on onward transfers which will review the use of the model contracts by the corporate group. The corporate group should make these contracts available to the data protection authorities upon request and to the data subjects on the conditions contained in the Commission decisions mentioned above.

3.3. Considerations about the binding nature of the corporate rules

Organisations respond to their data processing needs on the basis of different legal and cultural backgrounds and different business philosophies and practices. From the limited experience with these instruments, it is clear that nearly every multinational company approaches this matter in a different way. There is, however, an element that must be present in all systems if they are to be used to adduce safeguards for the data transfers to third countries: the binding nature of the corporate rules both internally and towards the outside world (legal enforceability of the rules).

3.3.1. Binding nature of the corporate rules within the corporate group[6]

A distinction can be made between the problem of compliance with the rules and the problem of their legal enforceability.

Indeed, the assessment of the "binding nature" of such corporate rules implies a common assessment of their binding nature *in law (legal enforceability)*, and of their binding nature *in practice (compliance)*. Even if the legal enforceability of unilateral commitments or contracts creating the same effects can be demonstrated from the conceptual perspective, the reality is that the enforcement of rights in transfrontier scenarios is always very complex and may involve disproportionate effort for the data subjects. Therefore, it is worth seeking not only that the internal rules are legally enforceable but also binding in practice[7].

The binding nature of the rules *in practice*, in this respect, would imply that the members of the corporate group, as well as each employee within it, will feel compelled to comply with the internal rules. In that respect, relevant elements could include the existence of disciplinary sanctions in case of contravention of the rules, individual and effective information of employees, setting up special education programmes for employees and subcontractors, etc. All these elements, which are also considered at section 5, could establish why individuals within the corporate group will feel obliged to comply with these rules.

---

[6] The adoption of a conduct is a step that corporations do not take lightly because its adoption poses significant risks and even legal consequences for those companies that breach their own code.

[7] WP 12 emphasises a functional approach and argues that the determining factor in relation to the adequacy is that the protection afforded is delivered in practice.

From the internal perspective, it is not for the Working Party to stipulate the way in which corporate groups should guarantee that all the members are effectively bound or feel compelled by the rules although some examples are well known such as internal policies whose application is of the responsibility of the headquarters or internal codes of conduct backed by intra company agreements[8]. But corporate groups must bear in mind that those applying for an authorisation will have to demonstrate to the grantor of the authorisation that this is effectively the case throughout the group.

The internal binding nature of the rules must be clear and good enough to be able to guarantee compliance with the rules outside the Community, normally under the responsibility of the European headquarters or the European member with delegated data protection responsibilities which must take any necessary measures to guarantee that any foreign member adjust their processing activities to the undertakings contained in the binding corporate rules.[9]

As a matter of fact, there is always an EU based member of the corporate group adducing sufficient safeguards and dealing with the application before the data protection authority. If the headquarters of the corporate group were somewhere else, the headquarters should delegate these responsibilities to a member based in the EU. It makes sense that the effective adducer of the safeguards remains responsible for the effective compliance with the rules and guarantees enforcement. See in this regard sections 5.5. and 5.6. on liability and jurisdiction.

3.3.2. Legal enforceability of the corporate rules by the data subjects (third party beneficiary rights) and by the data protection authorities

Data subjects covered by the scope of the binding corporate rules must become third party beneficiaries either by the legal effects of unilateral undertakings (where possible under national law) or by contractual arrangements between the members of the corporate group making this possible. As third party beneficiaries, data subjects should be entitled to enforce compliance with the rules both by lodging a complaint before the competent data protection authority and before the competent court on Community territory as explained later in section5.6.

The Article 29 Working Party attaches great importance to the existence of both possibilities. Although it seems much easier in principle for the data subject to lodge a complaint before the competent data protection authority and indeed the duty of co-operation of the corporate group with the authority is likely to solve most of the problems, there are two reasons that justify that, even in the assumption of a well-functioning system, the right to seek a judicial remedy is still necessary (see section 5.6):

a) because the duty of co-operation could never guarantee 100% compliance with the rules and data subjects may not necessarily always agree with the views of the data protection authority, and

---

[8] Ideally, the binding corporate rules should be adopted by the board of directors of the ultimate parent of the group.

[9] Under international corporate law affiliates may be able to enforce codes of conduct against each other based on claims of quasi-contractual breach, misrepresentation and negligence.

b) because the competence of data protection authorities in the Community can slightly vary from one country to the other (e.g. some authorities may not impose sanctions or block transfers directly) and none of them can award compensation for damages; only courts could do that.

Although the possibility for data subjects to enforce the rules before the courts is a necessary element for the reasons just mentioned, the Article 29 Working Party attaches more importance to the fact that the rules are complied with in practice by the corporate group as is the aim of any self-regulatory approach.

Regarding another aspect, differences in civil and administrative law raise the question of whether or not unilateral declarations can be regarded as the origin of third party beneficiary rights for individuals.

Where in some cases the legal enforceability of such unilateral declarations do not raise any doubts, in other Member States the situation is not that clear and unilateral declarations might not be sufficient as such. Where unilateral declarations cannot be considered as granting legally enforceable third party beneficiary rights, the corporate groups would have to put in place the necessary contractual arrangements allowing for that. These undertakings can be legally enforced under private law in all Member States. [10]

The scope of the third party beneficiary rights should match at least the one granted by the Commission Decision 2001/947/EC on standard contractual clauses in respect of both the Data Exporter and the Data Importer (see clause 3 "third-party beneficiary"[11]): this

---

[10] Nowadays it is possible to grant third party beneficiary rights in a contract in all Member States. See at this point previous experiences with standard contractual clauses and third party beneficiaries.

[11] Data subjects should be entitled to enforce the following rights (for ease of reference, corresponding clauses of the Commission Decision on Standard Contractual Clauses are indicated between brackets):

- that if the transfer involves special categories of data the data subject has been informed or will be informed before the transfer that this data could be transmitted to a third country not providing adequate protection (clause 4b)
- to obtain a copy of the binding corporate rules upon request (clauses 4c and 5e)
- to be replied to in a reasonable time and to the extent reasonably possible about queries concerning the processing of this personal data outside the Community (clauses 4d and 5c),
- to declare that a member of the corporation bound by the rules is not co-operating with the competent data protection authorities and/or is not abiding by the advice given by the data protection authority with regard to the processing of the data transferred (clause 5c),
- to declare that the legislation applicable to any of the members of the corporations outside the Community prevents him from fulfilling his obligations under the binding corporate rules (clause 5a)
- to declare that the processing of personal data of any member of the corporation bound by the rules is not in accordance with the binding corporate rules (clause 5b)
- to claim liability and, where appropriate, compensation in accordance with the terms set up in the binding corporate rules (clause 6),

clearly confirms the value and the importance of the existing standard contractual clauses.

Such contractual arrangements do not need to be complex or long. They are only instruments to trigger third party beneficiary rights for the individuals in those countries where there are doubts that unilateral declarations may achieve a similar result. In some cases, this could be achieved with the addition of a simple clause to other contracts in place between the members of the corporate group. For example, in those cases where there are contracts between the headquarters and the affiliates to guarantee internal compliance with the binding corporate rules -see previous section-, the addition of a "third party beneficiary clause" to them would be enough to meet this requirement.

As regards the legal enforceability of the binding corporate rules by the competent data protection authority, it is clear that by submitting an application for an authorisation for an international data transfer, the corporate group binds itself vis-à-vis the data protection authority to respect the safeguards adduced (in this case the binding corporate rules). This does not prejudice the question whether the responsibility to enforce these undertaking lies with the data protection authority herself or another authority (e.g. a court after the advice of the data protection authority).

On the top of that, data subjects would always be entitled to lodge a complaint before the national data protection authority or before judicial courts, as indicated under section 5.6 below. This might provide a more satisfactory course of action for data subjects and in any case a sort of "indirect" third party beneficiary rights for the data subjects.

3.3.3. Mandatory requirements of national legislation applicable to the members of the corporate group

The binding corporate rules should contain a clear provision indicating that where a member of the corporate group has reasons to believe that the legislation applicable to him may prevent him from fulfilling his obligations under the binding corporate rules and have a substantial adverse effect on the guarantees provided by them, he will promptly inform the headquarters in the EU or the EU member with delegated data protection responsibilities, unless otherwise prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

The headquarters in the EU or the EU member with delegated data protection responsibilities should take a responsible decision and have to consult the competent data protection authorities. Any incidences under this chapter of the rules will be detailed and reviewed by the regular audits foreseen under Chapter 5.2.

- to be able to use European jurisdiction in accordance with the terms set up in the binding corporate rules (clause 7),

- to declare that the rules have been varied contrary to the binding corporate rules or without respecting the procedural obligations set up thereof, or that any member of the corporation does not honour its obligations once he is no longer bound by the rules (clauses 9 and 11)

The scope of third party beneficiary rights must be clear in the contractual arrangements allowing for them.

Mandatory requirements of national legislation applicable to the members of the corporate group which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13 (1) of Directive 95/46/EC[12], are in principle not in contradiction with the binding corporate rules. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax reporting requirements or anti money-laundering reporting requirements. In case of doubt, corporate groups should promptly consult the competent data protection authority.

4. SUBSTANTIAL CONTENT OF THE BINDING CORPORATE RULES

4.1. Substantial content and level of detail

The Working Party reaffirms the principles contained in working document number 12[13], with special reference to chapters 3 (*applying the approach to Industry self-regulation*) and to a lesser extent chapter 6 (*procedural issues*). Having said that, it must be clear that these principles *per se* might mean very little for companies and employees processing personal data outside the Community, in particular in those countries where there is no data protection legislation in place and most probably no data protection culture whatsoever.

These principles need to be developed and detailed in the binding corporate rules so that they practically and realistically fit with the processing activities carried out by the organisation in the third countries and can be understood and effectively applied by those having data protection responsibilities within the organisation.

From this perspective, the binding corporate rules may have something in common with the codes of conducts foreseen in Article 27 of the Directive in the sense that they are supposed to overcome the level of abstraction of the legislation (in this case the principles of Working Document number12). The corporate rules should contain tailor-made provisions as well as a reasonable level of detail in the description of the data flows, purposes of the processing, etc.

As indicated in Article 26 (2) of the Directive, the authorisation may concern a transfer or a set of transfers but in any case there must be an explanation of the transfers being authorised. The level of detail must be sufficient so as to allow the data protection authorities to assess that the processing carried out in third countries is adequate (e.g. a detailed description of the economical activities pursued by the different entities of the corporate group).

---

[12] that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others

[13] Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.pdf

By way of example and in so far as the national applicable legislation provides for a notification regime, a practical suggestion could be that in those countries where the notification system contains a high level of detail, this section of the binding corporate rules should mirror the rules on the way that data controllers must notify to data protection authorities: in the same way that the notification allows the data protection authority to understand the processing operations carried out by the controller[14] the same level of information should in principle suffice for the data protection authority to understand the processing operations covered by the binding corporate rules within the corporate group. Where the level of detail in the notification system is not sufficiently detailed (Article 18.2 of the Directive gives Member States a great margin of manoeuvre in this regard), it would be necessary to add further information in order to provide an adequate description of the personal data being transferred to third countries. Binding corporate rules do not replace in any way notification requirements under EU law.

4.2. Particularisation and updates to the rules

Binding corporate rules may particularise further the relevant rules for different countries or regions outside the Community if this is the wish of the corporate group putting them in place. However, this particularisation would obviously add complexity to the system that is in principle meant to develop global policies.

As regards updates of the transfers taking place and, as matter of course, update of the rules, the Article 29 Working Party acknowledges that corporate groups are mutating entities whose members and practices may change from time to time and therefore they could not 100% correspond to the reality at the time the authorisation was granted. Updates are possible (without having to re-apply for an authorisation) providing that the following conditions are met:

a) no transfer of personal data is made to a new member until the exporter of the data has made sure that the new member is effectively bound by the rules and can deliver compliance,

b) an identified person or department of the corporate group should keep a fully updated list of the members and keep track of and record of any updates to the rules and provide the necessary information to the data subjects or data protection authorities upon request,

c) any updates to the rules or changes to the list of members should be reported once a year to the data protection authorities granting the authorisations with a brief explanation of the reasons justifying the update.

Updating the rules should be understood in the sense that working procedures may change and the rules would need to be adapted to such changing environments. Significant changes not only related to the principles of protection but also to the purposes of the processing, the categories of data processed or the categories of data subjects, would in principle have an effect on the authorisation.

[14] See Article 19 of the Directive

5. DELIVERING COMPLIANCE AND GUARANTEEING ENFORCEMENT

In addition to those rules dealing with substantial data protection principles, any binding corporate rules for international data transfers must also contain:

5.1. Provisions guaranteeing a good level of compliance

The rules are expected to set up a system which guarantees awareness and implementation of the rules both inside and outside the European Union. The issuing by the headquarters of internal privacy policies must be regarded only as a first step in the process of adducing sufficient safeguards within the meaning of Article 26 (2) of the Directive. The applicant corporate group must also be able to demonstrate that such a policy is known, understood and effectively applied throughout the group by the employees which received the appropriate training and have the relevant information available at any moment, for example via the intranet. The corporate group should appoint the appropriate staff, with top-management support, to oversee and ensure compliance.

5.2. Audits

The rules must provide for self-audits and/or external supervision by accredited auditors on a regular basis with direct reporting to the ultimate parent's board[15]. Data Protection Authorities will receive a copy of these audits where updates to the rules are notified and upon request where necessary in the framework of the co-operation with the data protection authority.

The rules must also indicate that the duty of co-operation with the data protection authorities (see chapter 5.4.) may also require the acceptance of audits to be carried out by inspectors of the supervisory authority themselves or independent auditors on behalf of the supervisory authority. This is most likely to be the case where the audits foreseen in the previous paragraph were not available for whatever reasons, they failed to contain relevant information necessary for a normal follow-up of the authorisation granted or the urgency of the situation would advocate in favour of a direct participation of the competent data protection authority or independent auditors on his behalf.

Such audits would take place in accordance with the relevant laws and regulations governing the data protection authorities' investigatory powers, without any prejudice to the inspection powers of each data protection authority, of which the corporate group will be duly informed by the competent data protection authority. In any case, they will take place with full respect to confidentiality and trade secrets and would be narrowly limited to ascertaining compliance with the binding corporate rules.

---

[15] The content of these audits must be comprehensive and elaborate in any case about some particulars already identified in this working document, such as the existence of onward transfers on the basis of standard contractual clauses (see section 3.2.) or the decisions taken as regards mandatory requirements under national law which may create conflicts with the binding corporate rules (see section 3.3.3.).

5.3. Complaint handling

The rules must set up a system by which individuals' complaints are dealt with by a clearly identified complaint handling department. Data protection officers or any person handling these complaints must benefit from an appropriate level of independence in the exercise of their functions. The use of alternative dispute resolution mechanisms, with the possible involvement of data protection authorities where appropriate, should also be promoted, in compliance with the applicable national laws and regulations.

5.4. The duty of co-operation with data protection authorities

As outlined in WP 12, one of the most important elements for assessing the adequacy of a self-regulatory system is the level of support and help available 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 personal data is not left alone, but is given some institutional support allowing his/her difficulties to be addressed"

This is indeed one of the most important elements of the binding corporate rules for international data transfers: the rules must contain clear duties of co-operation with data protection authorities so individuals can benefit from the institutional support mentioned in WP 12.

There must be an unambiguous undertaking that the corporate group as a whole and any of its members separately will accept the audit requirements indicated in chapter 5.2. There must also be an unambiguous undertaking that the corporate group as a whole and any of its members separately will abide by the advice of the competent data protection authority on any issues related to the interpretation and application of these binding corporate rules. The advice of the competent data protection authority will consist of recommendations addressed to the corporate group either in response to a questionnaire, as a result of a complaint lodged by a data subject or at the own initiative of the data protection authority.

Before issuing any advice the competent data protection authority may seek the views of the corporate group, the data subjects concerned and those data protection authorities which may be associated as a result of the co-ordinated procedure foreseen in this working document[16]. The advice of the authority may be made public.

In addition to any relevant provision at national level, a serious and/or persistent refusal by the corporate group to co-operate or to comply with the advice of the competent data protection authority may entail the suspension or the withdrawal of the authorisation granted either by the data protection authority itself or the competent authority under national law empowered to do so. This decision will have the form of an administrative act which the addressee may challenge before the competent court as provided for by national law. It will be notified to the European Commission and the other data protection authorities involved and it could also be made public.

---

[16] See chapter 6.

5.5. Liability

5.5.1. General right to obtain redress and where appropriate compensation

The rules should indicate that the data subjects would benefit from the remedies and liability provided for in Articles 22 and 23 of the Directive (or similar provisions transposing these articles of the Directive in the Member States legislations) in the same way and with the same scope from which they would benefit if the processing operation carried out by the corporate group would fall under the scope of the Data Protection Directive or any national laws transposing it.

The purpose of these rules therefore is limited to guaranteeing that authorisations granted by data protection authorities (which will make possible or lawful a transfer of personal data abroad which would otherwise be unlawful) would not end up depriving data subjects of their right to remedies or compensations from which they would have benefited had the data never left EU territory.[17]

As a complement to this general right, the rules must also contain provisions on liability and jurisdiction aimed at facilitating its practical exercise.

5.5.2. Rules on liability

First of all, the headquarters (if EU based) or the European member with delegated data protection responsibilities should accept responsibility for, and agree to take the necessary action to remedy the acts of other members of the corporate group outside the Community and, where appropriate, to pay compensation (within the scope indicated in the previous chapter) for any damages resulting from the violation of the binding corporate rules by any member bound by the rules.

The corporate group will attach to his request for an authorisation evidence that the EU headquarters or the European member with delegated data protection responsibilities has sufficient assets in the Community to cover the payment of compensation for breaches of the binding corporate rules in normal circumstances or that it has taken measures to ensure that it would be able to meet such claims to that extent (for example: insurance coverage for liability).

The headquarters (if EU based) or the European member with delegated data protection responsibilities must also accept that it will be sued in the EU and, where appropriate pay compensation:

a) in those cases where damages resulting from the breach of the binding corporate rules were claimed, or

---

[17] Some multinationals have been reluctant in the past to adopt global privacy policies on the argument that although they could agree to provide adequate protection to those covered by European legislation, they did not want to extend the same level of protection to other countries or regions where the level was not so high or there was no data protection at all. They have traditionally shown concern about the inclusion of any provisions on redress or compensation for data subjects. This formulation addresses these concerns, because as explained in Chapter 3.1.. the enforceability of the binding corporate rules (therefore including compensation for damages) may be limited to data originating from the EU.

b) damages were not claimed but the data subject was not satisfied with the remedies resulting from the recourse to the internal complaint handling procedures (see section 5.3.) or the lodging of a complaint before the competent data protection authority

Where the European headquarters or the European member with delegated data protection responsibilities can prove that the member of the corporate group in the third country is not responsible for the act resulting in the damage claimed by the data subject, it may discharge itself from any responsibility.

The rules should say that it would always be for the European headquarters or the European member with delegated data protection responsibilities to demonstrate that the member of the corporate group outside the Community is not liable for the violation resulting in the damage claimed by the data subject, rather than for the data subject to demonstrate that a company in a third country is engaged in processing contrary to the corporate rules (an evidence which most of the time would be impossible to get and in any case it would involve disproportionate effort, time and money for the data subject).

5.6. Rule on jurisdiction

As explained above in chapter 5.5.2., the corporate group must also accept that data subjects would be entitled to take action against the corporate group, as well as to choose the jurisdiction :

a) either in the jurisdiction of the member that is at the origin of the transfer, or

b) in the jurisdiction of the European headquarters or the jurisdiction of the European member with delegated data protection responsibilities.

Assuming the proper functioning of the system which implies a good level of compliance throughout the group, regular audits, efficient complaint handling, co-operation with data protection authorities, etc. the involvement of the courts seems unlikely, but in any case cannot be excluded. Having said that, only experience with these instruments will tell us if such forecast is right.

The relevant principles and rules on jurisdiction contained both in the Directive and in national laws will duly apply.

5.7. Transparency

In addition to the provision of information contained in Articles 10 and 11 of the Directive and national laws transposing them, corporate groups adducing sufficient safeguards must be in a position to demonstrate that data subjects are made aware that personal data are being communicated to other members of the corporate group outside the Community on the basis of authorisations by data protection authorities based on legally enforceable corporate rules, the existence and the content of which must be readily accessible for individuals.

This particularised duty to provide information means that without prejudice to the access to the corporate rules as a whole, corporate groups must be in a position to demonstrate that individuals have readily accessible information on the main data protection obligations undertaken by the corporate group, updated information as regards the members bound by the rules and the means available to data subjects in order to ascertain compliance with the rules.

6. PROCEDURE FOR CO-OPERATION BETWEEN NATIONAL AUTHORITIES WHEN DEALING WITH NATIONAL REQUESTS UNDER ARTICLE 26 (2) OF THE DIRECTIVE

The Working Party is aware of the importance of the notification of any authorisations granted to other Member States and to the European Commission as provided for in Article 26 (3) of the Directive. These notifications, nevertheless, may be complemented with additional co-operation activities between national data protection authorities before granting the relevant authorisations. Such a co-operation is indeed foreseen under Article 28 of the Directive in those cases where a national decision may have effects on the processing activities of the same corporate group in another Member State.

Corporate groups interested in a license for similar types of data export from several Member States may make use of a co-ordinated procedure[18]. Any coordinated activity applies only to those data protection authorities with powers under national law to authorise international data transfers and that are legally in the position to accept to be involved from time-by-time and on a case-by-case basis. .

The main idea behind this procedural arrangements is to allow companies to go through one process of application for a permit via a data protection authority of one Member State that will, through the co-ordination process between the involved data protection authorities, lead to the granting of permits by all the different DPAs of the Member States where this company operates. The details of the procedure will be promptly determined case-by-case by the data protection authorities involved.

This working document does not prejudice the rights and obligations that national supervisory authorities may have under national law to deal with complaints from individuals and, in general, to monitor the application of the Directive in those cases where they are competent. These arrangements, nevertheless, address the duty of co-operation provided for in Article 28 (6) of the Directive in those cases where they consider the legal pre-requisites at national level to co-operate with one another.

[18] The Article 29 Working Party may give further guidance on this issue as soon as possible and on the basis of the experience with this procedure. There is a co-operative working relationship between supervisory authorities in the Community therefore it is not necessary to provide for every eventuality. The applicant should indicate the entry point with an explanation of the grounds for its designation as well as the indication of other national supervisory authorities that should be involved in the procedure. The granting of the necessary authorisations under Article 26 (2) of the Directive and national laws pursuant to it and the notification to the European Commission would be the final steps of the co-ordinated procedure.

7. CONCLUSION

The Working Party believes that the guidance provided in this document may facilitate the application of Article 26 (2) of the Directive. It should also lead to a certain degree of simplification for multinational corporate groups routinely exchanging personal data on a world-wide basis.

The content of this working document should not be regarded as the final word of the Article 29 Working Party on this issue but as a solid first step to highlight the possibility to use national authorisations under Article 26 (2) on the basis of a self-regulatory approach and co-operation among the authorities, without prejudice to the possibility to use other tools for the transfer of personal data abroad such as the standard contractual clauses or the Safe Harbor principles where applicable.

Further input from interested circles and experts on the basis of the experience obtained with the use of this working document is welcomed. The Working Party might decide to revisit this issue in the light of experience.

Done at Brussels, 3 June 2003
For the Working Party
The Chairman
Stefano RODOTA