2093/05/EN
WP 114

Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995

Adopted on 25 November 2005

EXECUTIVE SUMMARY

This working document provides guidance as to how Article 26(1) of Directive 95/46 should be understood and applied by data controllers intending to initiate data transfers to countries which do not ensure an adequate level of protection, in the sense of Article 25 of the said Directive.

The Working Party issued this document to address its concern that differing interpretations are made of the provisions of Article 26(1) in practice, which prevent these provisions from being uniformly applied in the different Member States.

Similar concerns were voiced by the European Commission's report of 2003 on the implementation of Directive 95/46. The report recalled that neither an overly strict approach to the provisions of Article 25 and 26, nor an overly lax approach to those provisions (and then specifically those of Article 26 (1)) would be in line with their intended purposes, i.e. striking a fair balance between the protection of the individuals whose data are to be transferred to non adequate countries with, *inter alia*", the imperatives of international trade and the reality of global telecommunications networks".

In clarifying Article 26(1) derogations, among others by elaborating on Chapter 5 of working document WP12 on international data transfers which the group previously adopted in July 1998, this paper has sought to maintain the proper balance between the above mentioned interests

In Section 1 of this document, the Working Party sketches a general picture of how these provisions relate to others and together compose the global system of the Directive on international data transfers. It then provides elements of interpretation and recommendations which apply to the provisions of Article 26(1) as a whole. A central element of this interpretation is the necessity that the provisions of Article 26(1) must be strictly interpreted. Another element is that the derogations for the most part concern cases where risks to the data subject are relatively small or where other interests may be considered to override the data subject's right to privacy.

Section 1 further elaborates on this interpretation and expresses different recommendations which are designed to encourage controllers to ensure "adequate protection" in as many situations as possible.

In its Section 2, the document provides further guidance as to how each of the derogations of Article 26(1) must be interpreted. It specifically expands on the notions of "consent" and "performance of a contract", which are the derogations that controllers most often wish to rely upon in practice.

The Working Party believes that this document will be useful to clarify how data controllers may, and sometimes should make use of the derogations in Article 26 (1). The Working Party considers this document as an essential element of its policy on data transfers to third countries. This document should accordingly be read in conjunction with other work done by the Working Party in this domain, namely on "binding corporate rules", standard contractual clauses, and adequacy in third countries, including Safe Harbor.

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(1)(c) and (3) of that Directive,

Having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THIS WORKING DOCUMENT:

INTRODUCTION

The aim of this working document is to develop Chapter 5 of working document WP12 "Transfers of personal data to third countries: applying Articles 25 and 26 of the Directive", adopted by the Working Party on 24 July 1998[2], which relates to the interpretation of Article 26(1) of Directive 95/46/EC.

The provisions of Article 26(1) state that a data controller, subject to certain specified conditions, can transfer personal data to a third country by way of derogation from the principle of "adequate protection" laid down in Article 25 of the Directive.

In the light of the experience acquired since the document was adopted, the Working Party notes that there are differing interpretations of Article 26(1), which might prevent these provisions from being uniformly applied in the Member States.

This situation and the need for an appropriate reaction have also been noted by the Commission in the conclusions in its report on implementation of the Data Protection Directive[3]. The report underlines the significant divergences observed between the legislations of the various Member States in implementing Articles 25 and 26 of the Directive and the risk that this could ultimately lead to forum shopping among the Member States, depending on how loosely these provisions are interpreted[4]. This is borne out by the experience of certain national data protection authorities.

The Working Party therefore considers it necessary, in view of the tasks entrusted to it by Article 30(1)(a) of the Directive and in order to respond to the Commission's conclusions in the above-mentioned report, to specify the scope of these provisions and provide additional guidance for interpreting them.

---

[1] OJ L 281, 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/privacy/law_en.htm

[2] Working document 12/2001 "Transfers of personal data to third countries: Applying Articles 25 and 26 of the Data Protection Directive" of 24 July 1998.

[3] First report on the implementation of the Data Protection Directive (95/46/CE) of 15 May 2003, COM(2003) 265 final.

[4] Page 21 of the report: "An overly lax attitude in some Member States – in addition to being in contravention of the Directive – risks weakening protection in the EU as a whole, because with the free movement guaranteed by the Directive, data flows are likely to switch to the "least burdensome" point of export".

1. RELATIONSHIP BETWEEN THE DIFFERENT PROVISIONS OF DIRECTIVE 95/46 RELATING TO INTERNATIONAL TRANSFERS OF DATA, INCLUDING ARTICLE 26(1)

1.1 PRESENTATION OF THE PROVISIONS OF THE DIRECTIVE RELATING TO INTERNATIONAL DATA TRANSFERS TO THIRD COUNTRIES

When interpreting Article 26(1) of Directive 95/46/EC it is necessary to bear in mind the general framework for these provisions in order to ensure a consistent interpretation of the provisions of the Directive relating to international transfers of data.

Directive 95/46/EC of 24 October 1995 provides different legal bases for transfers of personal data to third countries, including those laid down in Article 26(1):

1. Adequacy in recipient country: first and foremost, Article 25(1) lays down the general principle, according to which "the transfer to a third country of personal data […] may take place only if […] the third country in question ensures an adequate level of protection". The level of data protection should be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations, and giving particular consideration to a number of elements relevant for the transfer and listed in Article 25(2).

   In line with Article 249 TEC, the directive is binding upon each Member State to which it is addressed as to the result to be achieved, while it leaves to the national authorities the choice as to how this result should be achieved. In this regard, the directive imposes on Member States an obligation to make sure that personal data is not transferred to a third country unless it guarantees an adequate level of protection, and provides that the assessment of adequacy is done in the light of all the circumstances. The directive does not specify, however, whether an authority should be charged with assessing the adequacy of data protection in third countries. It is therefore possible that national legislation in Member States endows this task on national data protection authorities, whose authorisation may be required for the transfer of personal data to a third country to take place.

   Beside this possibility for national authorities to assess adequacy as allowed by national legislation, the Directive provides for Europe-wide decisions on adequacy to be adopted by the Commission, thus providing an added value of legal certainty and uniformity throughout the Community. Under Article 25(6) the Commission may recognise that certain countries offer adequate protection, in which case transfers of personal data may take place to these countries without needing to fulfil any specific formal requirement. This now applies to international transfers of data to recipients established in Switzerland, Canada, Argentina, Guernsey or the Isle of Man, or when the recipient is an American enterprise that has signed up to Safe Harbor[5]. This legal basis was also used as a basis for the transfer to the United States' Bureau of Customs and Border Protection of Passenger Name Records concerning flights to or from the United States, pursuant to a Commission decision on which this Working Party has been very critical.

[5] Information on these countries and on the Safe Harbor system are available on the following website: http://europa.eu.int/comm/internal_market/privacy/adequacy_fr.htm

2. Adequate safeguards put in place by recipient: secondly, under Article 26(2) of the Directive a Member State may also authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection where the data controller offers "adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights".

   The end of Article 26(2) also states that these safeguards "may in particular result from appropriate contractual clauses". To facilitate the use of contractual clauses, the European Commission has issued three decisions on standard contractual clauses, two of which regulate transfers from a data controller to a data controller while the third regulates transfers from a data controller to a processor[6].

   In addition, apart from the possibility of using contractual clauses to provide such sufficient safeguards, since 2003 the Article 29 Working Party has been working actively on the possibility of multinational groups using "binding corporate rules" for the same purpose[7].

3. Derogations of Article 26(1): thirdly, Article 26(1) of the Directive states that transfers of personal data to a third country which do not ensure an adequate level of protection may take place if one of the following conditions is met :

   a) the data subject has given his consent unambiguously to the proposed transfer;

   b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;

   c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;

   d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;

   e) the transfer is necessary in order to protect the vital interests of the data subject;

   f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

In the cases listed in sections 1 and 2 above, the transfer takes place under conditions that ensure that the individuals in question continue to be protected as regards processing of their data, once the data have been transferred. This protection is provided either by the

[6] As regards transfers from a data controller to a data controller, the Commission issued a first set of standard contractual clauses on 15 June 2001; it subsequently amended this decision in order to annex a new set of alternative clauses (decision of 27 December 2004). With regard to transfers from a data controller to a processor, the Commission issued a set of standard contractual clauses on 27 December 2001. All these clauses are available on the following website:
http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm

[7] Cf. working document WP 74, "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 by the Working Party on 3 June 2003 and further complementary documents WP107 and WP108.

general legislation or sectoral rules in force in the country in which the recipient is established, or by adequate safeguards provided by the data controller in the Community, in particular in view of binding commitments undertaken by the recipient as regards processing of the data transferred to this third country.

Conversely, Article 26(1) contains genuine derogations from the principle of adequate protection laid down in Article 25 of the Directive. In fact, these exceptions allow the transfer to take place to third countries that do not ensure an adequate level of protection. *A fortiori*, they could also be used as a legal basis where the country does ensure an adequate level of protection but where its adequacy has not been assessed. Although the use of the derogations *per se* does not imply in all cases that the country of destination does not ensure an adequate level of protection, it does not ensure that it does either. As a consequence, for an individual whose data have been transferred, even if he has consented to the transfer, this might imply a total lack of protection in the recipient country, at least in the sense of the provisions of Article 25 or 26(2) of directive 95/46.

Considering this important difference in terms of protection, it is important that these various legal bases are implemented consistently with respect to the overall system of which they form part.

1.2 THE POSITION OF ARTICLE 26(1) IN THE SYSTEM OF THE DIRECTIVE

The juxtaposition of these different rules on transfers of personal data may give a paradoxical impression, and can easily give rise to misunderstanding.

On the one hand, a first set of provisions, those contained in Articles 25(1), 25(6) and 26(2), aim at ensuring that the personal data transferred will continue to enjoy appropriate protection after it has been transferred to the country of destination. These transfers may take place either because the legal framework of the third country in question provides for an adequate protection, or because such protection is guaranteed by standard contractual clauses or by other kinds of adequate safeguards, such as the conclusion of a contract, the adoption of BCRs, self-certification to comply with the Safe Harbor principles, etc. On top of this, as was mentioned earlier, a certain number of national legislations provide that some transfers may also be subject to an authorisation or a prior opinion to be obtained from the relevant national authorities (in most cases, the data protection authorities).

On the other hand, a second set of provisions, those contained in Article 26(1), make it substantially easier to transfer personal data to a third country. Under these provisions, the data controller originating the transfer neither has to make sure that the recipient will provide adequate protection nor usually needs to obtain any kind of prior authorisation for the transfer from the relevant authorities, if this procedure would be applicable. Furthermore, these provisions do not require the data recipient to comply with the Directive requirements as regards any processing of the data in his own country (e.g. principles of purpose, security, right of access, etc.).

The literal wording of the Directive might lead one to the conclusion that there is considerable lack of consistency in its provisions on transfers of personal data to third countries. After all, the rationale of the principle of adequate protection, enshrined in Article 25, consists in ensuring that individuals should continue to benefit from the

fundamental rights and freedoms which they are granted in relation to the processing of their data in the European Union once these data have been transferred to a third country. It also aims at preventing that the protection provided by European personal data protection legislation be circumvented by the fact of transferring the data to third countries.

One explanation for such apparent duality of principles is the acknowledgement that the expansion of international trade requires on certain occasions flexibility of international data transfers, including transfers of personal information (as set out in Recital 56 of the Directive).

Another explanation of this apparent lack of consistency can be found, however, if one realises that Article 26(1) was designed to deal with a limited number of situations in which an exemption from the "adequacy" requirement for third country transfers was considered to be appropriate. As the Working Party already mentioned in document WP12: "These exemptions, which are tightly drawn, for the most part concern cases where risks to the data subject are relatively small or where other interests (public interests or those of the data subject himself) override the data subject's right to privacy. As exemptions from a general principle, they must be interpreted restrictively. Furthermore, Member States may provide in domestic law for the exemptions not to apply in particular cases. This might be the case, for example, where it is necessary to protect particularly vulnerable groups of individuals, such as workers or patients."

In practice, however, there has been a tendency among controllers to make use of these exemptions as a first option, even where this would be inappropriate.

Therefore, the Working Party would first of all like to ensure that the scope and meaning of Article 26(1) are well understood by all those concerned to avoid the use by controllers of the derogations in inappropriate cases. This requires a clear and common interpretation of Article 26(1) itself, and of its position in the Directive as a whole.

This exercise must be led by the rule that, as previously indicated by the Working Party in its working document WP12 mentioned above, the interpretation of Article 26(1) must necessarily be strict.

In this respect, the Working Party emphasises that this logic is the same as that of the additional protocol to Convention 108. The report on this protocol states that "the parties have discretion to determine derogations from the principle of an adequate level of protection. The relevant domestic provisions must nevertheless respect the principle inherent in European law that clauses making exceptions are interpreted restrictively so that the exception does not become the rule".[8]

More generally, this rule of strict interpretation also clearly derives from the case law of the European Court of Human Rights which interprets fundamental rights in quite a wide manner, in accordance with the so-called *"principe d'effet utile"* of the protection awarded, to the effect of limiting the scope of the derogations to this principle. The Court has used this principle in several landmark cases[9].

[8] Cf. report on the Additional Protocol to Convention 108 on the control authorities and crossborder flows of data, Article 2(2)(a); this document can be accessed at:
http://conventions.coe.int/Treaty/EN/Reports/Html/181.htm

[9] Cases Delcourt (17 January 1970) and Klass (6 September 1978)

The Working Party therefore explicitly confirms its understanding of Article 26(1) as previously indicated, and explains this interpretation in more detail in Section 2 of this working document.

It should also be noted, however, that the provisions of the Directive relating to transfers of personal data to third countries cannot be applied separately from other provisions of the Directive. As explicitly mentioned in Article 25(1), these provisions apply "without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive". This means that regardless of the provisions relied upon for the purpose of data transfer to a third country, other relevant provisions of the Directive need to be respected.

This specifically means, in accordance with Paragraph 60 of the Preamble of the Directive, that where sensitive data is involved in the transfer, the requirements of Article 8 of the Directive need to be satisfied. This may imply that a specific transfer can only rely on Article 26(1) - where applicable - if the conditions of Article 8 are fulfilled. In other words, even if national law did not make use of the possibility to restrict the scope of Article 26(1) for certain categories of cases, there may still be additional restrictions resulting from other provisions of the Directive.

The Working Party would also like to mention that the principles of "fair, lawful processing", and "compatible use", as laid down in Article 6(1) sub a and b, continue to apply in this context. This may imply that the controller has a duty to inform data subjects about relevant details of data transfers to a third country, even where this would not be required by Articles 10, 11 or 26(1). In the same manner, it may happen that a data subject has a reason to object to specific transfers "on compelling legitimate grounds relating to his particular situation", as provided in Article 14 sub a, of the Directive. This may also relate to personal data that are not sensitive in the sense of Article 8 of the directive or in the sense of what the data subject might consider as sensitive data about him/herself in a given situation (e.g. financial data, data enabling an adverse decision being taken against the data subject in terms of company management, etc.).

1.3 RECOMMENDATIONS ON THE RESPECTIVE USE OF THE DIFFERENT LEGAL GROUNDS PROVIDED BY THE DIRECTIVE FOR INTERNATIONAL DATA TRANSFERS

Furthermore, without prejudice to the general interpretation of Article 26(1) in point 1.2 of this working document nor to the specific interpretation of each derogation in Section 2 below, the Working Party would like to make a number of recommendations on the respective use of the different legal grounds provided by the Directive for data transfers to third countries.

These recommendations are elaborated in Chapter 5 of document WP12. They are designed to encourage controllers to ensure "adequate protection" in as many situations as possible. The Working Party has already held that when planning to transfer data to a third country, data controllers established in the European Union should favour solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards to which they are entitled as regards processing of their data in the EU once this data has been transferred.

Accordingly, a best practice approach would be for a data controller planning an international data transfer to consider first whether the third country provides an adequate level of protection and to satisfy himself that the exported data will be safeguarded in that country. In the case of exports to the US, the controller exporter may want to encourage the importer to subscribe to the Safe Harbor principles. If the level of protection in the third country is not adequate in the light of all the circumstances surrounding a data transfer, the data controller should consider Article 26(2), i.e., providing adequate safeguards through, for example, the standard contractual clauses or binding corporate rules. Only if this is truly not practical and/or feasible, then the data controller should consider using the derogations of Article 26(1).

Further in line with this logic, the Working Party would recommend that the derogations of Article 26(1) of the Directive should preferably be applied to cases in which it would be genuinely inappropriate, maybe even impossible for the transfer to take place on the basis of Article 26(2).

The Working Party would find it regrettable that a multinational company or a public authority would plan to make significant transfers of data to a third country without providing an appropriate framework for the transfer, when it has the practical means of providing such protection (e.g. a contract, BCR, a convention).

It is in particular for this reason that the Working Party would recommend that transfers of personal data which might be qualified as repeated, mass or structural should, where possible, and precisely because of these characteristics of importance, be carried out within a specific legal framework (i.e. contracts or binding corporate rules). The Working Party acknowledges, on the other hand, that there will be cases where mass or repeated transfers can legitimately be carried out on the basis of Article 26(1), when recourse to such a legal framework is impossible in practice, where the risks to the data subject are small and Articles 6, 7 and 8 applied appropriately. One relevant example is for instance provided by international money transfers which still take place daily, and in a massive way.

Thus, even in certain cases where the legitimacy of the transfer would result from one of the cases listed in Article 26(1), the Working Party would recommend that additional factors such as the size of the planned transfer or the risks induced for the data subjects should lead the controller to conclude a contract or develop BCRs in order to carry it out.

Finally, recourse to the derogations of Article 26(1) should of course never lead to a situation where fundamental rights might be breached.

When it introduced these derogations to the principle of adequate protection in the Directive, the European lawmaker considered these derogations to be justified insofar as they were considered compatible with the protection of individuals' fundamental rights and the free international flow of information. In other words, while the cases listed in Article 26(1) may constitute a derogation to the principle that the third country should guarantee an adequate protection, they do not provide additional exemptions from the rule that fundamental rights should be respected.

The national data protection authorities should ensure that these derogations are applied in situations that do not entail a breach of the data subjects' fundamental rights and

which correspond to the need to maintain a strict interpretation of these derogations. In this respect, the authorities can, if there is sufficient reason to do so, intervene at any time and recommend that an international transfer of data should be carried out on the basis of adequate safeguards in the meaning of Article 26(2) rather than by applying the exceptions listed in Article 26(1).

2. SPECIFIC INTERPRETATION OF THE PROVISIONS OF ARTICLE 26(1)

In addition to the general comments made in the previous Section, the Working Party also wishes to provide some guidelines as to the specific meaning of each of the derogations listed in Article 26(1). These guidelines were elaborated on the basis of the Working Party's experience and that of the national personal data protection authorities in this area, and on the basis of the understanding that the wording of the derogations be given their natural meanings, i.e. be neither artificially constrained nor artificially extended.

2.1 CONSENT (ARTICLE 26(1)(a))

Article 26(1)(a) states that a transfer of personal data may be made to a country which does not ensure an adequate level of protection on condition that "the data subject has given his consent unambiguously to the proposed transfer".

As already indicated in the Working Party's previous working document WP 12, an important point is that in order to be valid, this consent, whatever the circumstances in which it is given, must be a freely given, specific and informed indication of the data subject's wishes, as defined in Article 2(h) of the Directive.

- Consent must be a clear and unambiguous indication of wishes

The importance of consent constituting a positive act excludes *de facto* any system whereby the data subject would have the right to oppose the transfer only *after* it has taken place: specific consent to a transfer must genuinely be required for the transfer to take place. Any doubt as to whether consent has really been given would make the derogation inapplicable. Thus, as the Working Party states in its document WP12, "this is likely to mean that many situations where consent is implied (for example because an individual has been made aware of a transfer and has not objected) would not qualify for this exemption".

Furthermore, in its opinion on the interpretation of Article 13 of the directive on privacy and electronic communications[10], which introduced a uniform system for direct marketing communications to individuals, the Working Party provided guidance on interpretation of the concept of "prior consent" in the specific context of electronic communications, and in particular on the Internet. It is helpful to refer to this guidance in the present document, since the data subject's consent to a transfer may sometimes be requested online. In particular, the Working Party recommended the use on Internet sites of boxes to be ticked by the data subject as an indication of his prior consent; using pre-ticked boxes fails to fulfil the condition that consent must be a clear and unambiguous indication of wishes.

[10] Opinion 5/2004 on unsolicited direct marketing communications under Article 13 of Directive 2002/58/EC, WP 90, of 27 February 2004, point 3.2.

- Consent must be given freely

Consent given by a data subject who has not had the opportunity to make a genuine choice or has been presented with a *fait accompli* cannot be considered to be valid.

For this reason, the Working Party has discussed whether consent can be validly used to transfer booking details ("PNR data") of European airlines to the U.S. authorities. It was indeed questionable whether passengers' consent could have been given freely as the airlines are obliged to send the data before the flight departure, and passengers therefore had no real choice if they wished to fly[11].

On this point, the Working Party wishes to draw attention to the fact that specific difficulties might occur to qualify a data subject's consent as freely given in an employment context, due to the relationship of subordination between employer and employee[12]. Valid consent in such a context means that the employee must have a real opportunity to withhold his consent without suffering any harm, or to withdraw it subsequently if he changes his mind. In such situations of hierarchical dependence, an employee's refusal or reservations about a transfer might indeed cause him non-material or material harm, which is completely contrary to the letter and spirit of European personal data protection legislation. The Working Party acknowledges, however, that there will be cases where it is appropriate for an employer to rely upon consent, for example, in an international organisation where employees wish to take advantage of opportunities in a third country.

In this light, the Working Party would invite employers not to rely solely on their employees' consent when transferring their data, apart from in cases in which it is established employees would not suffer any consequences if they wished not to give their consent to a transfer, or if they did give their consent but subsequently wished to withdraw their consent, in cases where this would be possible.

Furthermore, in the light of experience, the Working Party suggests that consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question. In fact, particularly if the transfer forms an intrinsic part of the main processing (e.g. centralisation of a world database of human resources, which needs to be fed by continual and systematic data transfers to be operational), the data controllers could find themselves in insoluble situations if just one data subject subsequently decided to withdraw his consent. Strictly speaking, the data relating to a person who had withdrawn his consent could no longer be transferred; failing this, the transfer would continue to be partially based on the data subject's consent, but an alternative solution (a contract, BCR, etc.) would have to be found for data relating to subjects who had withdrawn their consent. Relying on consent may therefore prove to be a "false good solution", simple at first glance but in reality complex and cumbersome.

[11] Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States.

[12] Opinion 8/2001 on the processing of personal data in the employment context and executive summary, dated 13 September 2001.

- Consent must be specific

In addition, to constitute a valid legal basis for a possible transfer of data, the data subject's consent must be specifically given for the particular transfer or a particular category of transfers in question.

Since consent must be specific, it is sometimes impossible to obtain the data subject's prior consent for a future transfer, e.g. if the occurrence and specific circumstances of a transfer are not known at the time consent is requested and so the impact on the data subject cannot be assessed. To cite an example, a company, when obtaining its customers' data for a specific purpose, cannot ask them to give their prior consent to the transfer of their data to a third country in the event of the company being taken over by a third company. However, it is possible to envisage that a person may validly consent to the transfer of his data to a third country in advance, when the details of the transfer are already predetermined, notably in terms of purpose and categories of recipients.

- Consent must be informed

This condition is particularly important. It requires the data subject to be properly informed in advance of the specific circumstances of the transfer (its purpose, the identity and details of the recipient(s), etc.) in accordance with the general principle of loyalty.

The information given to data subjects must also include the specific risk resulting from the fact that their data will be transferred to a country that does not provide adequate protection. Only this information will enable the data subject to consent with full knowledge of the facts; if it is not supplied, the derogation will not apply.

The Working Party has observed that it is sometimes complicated to obtain consent for practical problems, in particular where there is no direct contact between the data controller and the data subjects (although the solution provided for in Article 26(2) sometimes proves to be easier to implement). Whatever the difficulties, the data controller must be able to prove in all cases that, firstly, he has obtained the consent of each data subject and, secondly, that this consent was given on the basis of sufficiently precise information, including information on the lack of protection in the third country.

2.2 TRANSFER NECESSARY FOR PERFORMANCE OF A CONTRACT BETWEEN THE DATA SUBJECT AND THE CONTROLLER OR FOR THE IMPLEMENTATION OF PRECONTRACTUAL MEASURES TAKEN IN RESPONSE TO THE DATA SUBJECT'S REQUEST (ARTICLE 26(1)(b))

In its working document WP12, the Working Party stated that although the scope of these derogations relating to performance of the contract appears to be potentially very broad, in practice it will be limited by the criterion of "necessity".

In fact, the Working Party is aware that, irrespective of the general interpretation of Article 26(1) and of the further recommendations mentioned in Section 1.3 of this document, this "necessity test" as such might limit the number of cases in which recourse can be made to the different derogations of Article 26(1) which refer to this notion of "necessity" (Article 26(1) sub b to sub e).

In the case of Article 26(1)(b), a transfer of data to a third country that does not provide adequate protection can only be deemed to fall under the exception in Article 26(1)(b) if it can be considered to be *necessary* for the performance of the contract in question or for the implementation of precontractual measures taken at the data subject's request. This "necessity test" here requires a close and substantial connection between the data subject and the purposes of the contract.

Thus, certain international groups would like to be able to avail themselves of this exception in order to transfer data of their employees from a subsidiary to the parent company, for example in order to centralise the group's payment and human resources management functions. They believe that such transfers could be deemed necessary for performance of the employment contract concluded between the employee and the data controller. The Working Party holds this interpretation as excessive since it is highly questionable whether the concept of an employment contract can be interpreted so broadly, as there is no direct and objective link between performance of an employment contract and such a transfer of data.

Furthermore, a strict interpretation of this exception means that the data transferred must be truly necessary to the purpose of the performance of this contract or of these precontractual measures.

For this reason, in its PNR opinion of 24 October 2002 the Working Party refused to take the view that this condition could be applied to transfers of data of air passengers to the U.S. authorities, due to the scope of the data transferred, certain of which cannot be deemed "necessary" for performance of the transport contract[13].

On the contrary, this derogation would be an acceptable legal basis for the transfer by travel agents of personal data concerning their individual clients to hotels or to other commercial partners that would intervene in the organisation of these clients' stay.

Finally, this derogation cannot be applied to transfers of additional information not necessary for the purpose of the transfer, or transfers for a purpose other than the performance of the contract. More generally, the derogations of Article 26(1)(b) to (e) only allow that the data which are necessary for the purpose of the transfer may be transferred on the basis of the individual derogations; for additional data, other means of adducing adequacy should be met.

2.3 TRANSFER NECESSARY FOR THE CONCLUSION OR PERFORMANCE OF A CONTRACT CONCLUDED IN THE INTEREST OF THE DATA SUBJECT BETWEEN THE CONTROLLER AND A THIRD PARTY (ARTICLE 26(1)(c))

The interpretation of this provision is necessarily similar to the preceding one, namely that a transfer of data to a third country which does not ensure adequate protection cannot be deemed to fall within the exception contained in Article 26(1)(c) unless it can be considered to be truly "necessary for the conclusion or performance of a contract between the data controller and a third party, in the interest of

[13] Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States.

the data subject", and pass the corresponding "necessity test". In the present case, this test requires a close and substantial connection between the data subject's interest and the purposes of the contract.

Some data controllers have sometimes expressed the wish to have recourse to this derogation as a basis for international data transfers concerning their employees to providers, established outside the EU, to which they outsource their payroll management. According to them, such transfers would be necessary to the performance of their outsourcing contract, and would be in the interest of the data subject since the finality of the transfer is the management of the pay of the employee. In this case, however, the Working Party believes that the close and substantial link between the data subject's interest and the purposes of the contract is not established, and that the derogation cannot apply.

Also, certain international groups would like to be able to apply this exception when managing stock option schemes for certain categories of their employees. To do this, these groups classically use the services of financial service-providers, specialising in the management of such schemes, established in third countries. The groups consider that transfers could thus be made to this service provider for the purpose of performing the contract concluded between the provider and the data controller, in the interest of the beneficiaries of the scheme.

If a data controller was to rely on Article 26(1)(c) as a basis for these arrangements, as the Working Party has its reservations about the validity of this interpretation, a data controller would have to satisfy a data protection authority that the data transferred is necessary for the performance of that contract in accordance with the strict interpretation of "necessary" referred to above.

The Working Party wants to make clear that this interpretation by no means implies that it bears a negative judgement on the choice by controllers to have recourse to data processors in third countries. It simply wishes to insist on the appropriateness of relying on an Article 26(2) instrument (in practice, a contract) to initiate data transfers in such cases.

2.4 TRANSFER NECESSARY OR LEGALLY REQUIRED ON IMPORTANT PUBLIC INTEREST GROUNDS, OR FOR THE ESTABLISHMENT, EXERCISE OR DEFENCE OF LEGAL CLAIMS (ARTICLE 26(1)(d))

The exceptions in Article 26(1)(d) must be interpreted using the same strict criterion as that applied in the previous paragraphs.

The Working Group has already given a restrictive interpretation of the concept of "important public interest grounds" in its PNR opinion of 24 October 2002[14]. It rejected the use of this exception to justify transfers of data of airline passengers to the U.S. authorities on important public interest grounds for two reasons: firstly, the necessity of the transfer had not been established, and secondly, it did not appear acceptable for a

[14] Opinion 6/2002 referred to above.

unilateral decision by a third country, on public interest grounds specific to it, to lead to regular bulk transfers of data protected by the Directive.

On this point the drafters of the Directive clearly did envisage that only important public interests identified as such by the national legislation applicable to data controllers established in the EU are valid in this connection. Any other interpretation would make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country laid down in Directive 95/46.

On the other hand, Recital 58 of Directive 95/46 refers, with regard to this provision, to cases in which international exchanges of data might be necessary "between tax or customs administrations in different countries" or "between services competent for social security matters". This specification, which appears to relate only to investigations of particular cases, explains the fact that this exception can only be used if the transfer is of interest to the authorities of an EU Member State themselves, and not only to one or more public authorities in the third country.

The Working Party emphasises that the concept of "establishment, safeguarding or defence of legal claims" must here again be subject to strict interpretation. Thus, for example, the parent company of a multinational group, established in a third country, might be sued by an employee of the group currently posted to one of its European subsidiaries. The exception in Article 26(1)(d) appears to allow the company to legally request the European subsidiary to transfer certain data relating to the employee if these data are necessary for its defence.

In any event, this exception cannot be used to justify the transfer of all the employee files to the group's parent company on the grounds of the possibility that such legal proceedings might be brought one day.

In addition, this exception can only be applied if the rules governing criminal or civil proceedings applicable to this type of international situation have been complied with, notably as they derive from the provisions of the Hague Conventions of 18 March 1970 ("Taking of Evidence" Convention)[15] and of 25 October 1980 ("Access to Justice" Convention)[16].

2.5 TRANSFER NECESSARY IN ORDER TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT (ARTICLE 26(1)(e))

The exception in Article 26(1)(e) obviously applies when data are transferred in the event of a medical emergency, where they are considered to be directly necessary in order to give the medical care required.

Thus, for example, it must be legally possible to transfer data (including certain personal data) if the data subject is unconscious and in need of urgent medical care, and only his usual doctor, established in an EU country, is able to supply these data. In such cases it would be absurd to impose any other type of requirement for legally transferring the data.

[15] Hague Convention of 18 March 1970 on the taking of evidence in civil and commercial matters
[16] Hague Convention of 25 October 1980 on international access to justice

The transfer must relate to the individual interest of the data subject and, when it bears on health data, it must be necessary for an essential diagnosis. Accordingly, this exception could not be used to justify transferring personal medical data to persons responsible for treatment and established outside the EU if their purpose is not to treat the particular case of the data subject but, for example, to carry out general medical research that will not yield results until some time in the future. In these cases, the alternative requirements laid down in Article 26(2) of the Directive would have to be met.

2.6 TRANSFER MADE FROM A PUBLIC REGISTER (ARTICLE 26(1)(F))

The exception in Article 26(1)(f) concerns transfers "from a public register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case".

This provision of the Directive is a logical consequence of the open nature of the registers referred to, which can be freely consulted. If such a register can be consulted by anyone in the country or by any person with a legitimate interest in doing so, it seems logical to allow it to be consulted by a person established in a third country.

However, this freedom to transfer data cannot be total. Recital 58 of the Directive states that "in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register". It would not be in keeping with the spirit of Article 26(1)(f) if this legal ground for transfer was used to empty these registers of their content, with the risk that their use by entities established in third countries could ultimately lead them to be used for purposes other than that for which they were originally set up.

In addition, recital 58 states that "when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients". One could imagine that this exception might be used, national laws abiding, by a person born in an EU Member State but resident in a third country in order to obtain extracts of his certificates of civil status from his place of birth in order to take up permanent residence in his new country of residence.

In any case, reference will have to be made to the laws and regulations of the EU Member State in which the register was set up in order to verify whether this exception can apply in certain specific cases. In particular, these laws and regulations will define the concepts of "intended to provide information to the public" and "legitimate interest" based on which the exception might be used.

3. CONCLUSION

As stated in the introduction, the aim of this working document is to provide guidance in interpreting the derogations in Article 26(1) of Directive 95/46/CE of 24 October 1995.

In the present document, the Working Party upholds its previous interpretation, set forth in its working document WP12, that all the derogations listed in Article 26(1) must be interpreted strictly.

However, in the context of an acceleration of international data transfers over the recent years, which the daily practice of national data protection authorities shows as obvious, the Working Party finds it necessary to provide further elements of recommendations as to the application of these provisions.

In so doing, the Working Party is particularly sensitive to the concern that the various legal grounds which the directive offers as a basis for international data transfers should be used in a coherent manner, and in any case in a way that does not undermine the principle of adequate protection which is enshrined in Article 25 of the directive.

In this respect, the Working Party recommends that the present document be read in conjunction with the other documents which it has previously adopted in the area of international data transfers, and notably document WP74.

The Working Party expresses the wish that data controllers make use of the derogations of Article 26(1) in accordance with the recommendations set forth in the present document.

Done at Brussels,

For the Working Party
The Chairman
Peter Schaar