Ref. Ares(2011)1347128 - 13/12/2011

**ARTICLE 29 DATA PROTECTION WORKING PARTY**

Brussels, 13 December 2011

Mr Jonathan FAULL
Director General
Internal Market & Services DG
European Commission
200 Rue de la Loi
B-1049 Brussels

Dear Madam, Dear Sir,

The Article 29 Working Party (the WP 29) was requested to provide guidance to the auditing unit of DG MARKT[1] on the application of Directive 95/46 in relation to the international transfer of personal data to the US Public Company Accounting Oversight Board (PCAOB)[2], the application of Directive 2006/43[3] and the Commission Decision 2010/485/EU of 1 September 2010[4] (the Commission Decision).

As you know, the WP 29 has already adopted an opinion on the Directive 2006/43[5].The WP 29 now understands that the PCAOB contacted several oversight authorities of the Member States directly last year in order to conclude non-binding bilateral arrangements to enhance cooperation, including the exchange of personal data under audit reports and working documents of audit firms. For instance, on 10 January 2011, the PCAOB *"entered into a cooperative agreement with the Professional Oversight Board in the United Kingdom to facilitate cooperation in the oversight of auditors and public accounting firms that practice in the two regulators' respective jurisdictions."*[6]

[1] Subgroup Financial Matters of 24 June 2011.

[2] According to its website http://pcaobus.org/Pages/default.aspx , the PCAOB is a nonprofit corporation established by Congress to oversee the audits of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, accurate and independent audit reports. The PCAOB also oversees the audits of broker-dealers, including compliance reports filed pursuant to federal securities laws, to promote investor protection.

[3] Directive of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC, O.J., 9 June 2006, published on http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0087:0087:EN:PDF

[4] Commission Decision of 1 September 2010 on the adequacy of the competent authorities of Australia and the United States pursuant to Directive 2006/43 of the European Parliament and of the Council, notified under document C(2010) 5676, OJ 11 September 2010, published on http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:240:0006:0009:EN:PDF

[5] Opinion WP 143 of 23 November 2007.

[6] http://pcaobus.org/News/Releases/Pages/01102011_UK.aspx

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

The WP 29 was informed that similar discussions to adopt bilateral agreements are still ongoing in other countries including, but not limited to, Germany, Spain, Belgium and the Grand Duchy of Luxembourg. The oversight authorities of these countries have requested specific and practical data protection guidance in the last six months, usually by directly referring to the competent DPA.

The WP 29 has made an additional assessment and made some recommendations which you will find attached to this letter as annexes (annex 1 contains the WP 29's understanding of the issue and a legal analysis, whilst annex 2 contains practical recommendations.)

The WP29 finds that a harmonized EU approach would be preferable, as it offers more effective data protection and legal certainty for all stakeholders across Europe than is offered by the current bilateral approach. The WP 29 would like to work with the European Commission (the Commission) and the European Group of Audit Oversight Boards (EGAOB) to take a more comprehensive look at this and resolve some of the issues identified.

We hope that the recommendations and the offer of further assistance are both helpful and accepted. I look forward to receiving your reply.

Yours faithfully,

For the Working Party
*The Chairman*
Jacob KOHNSTAMM

Cc: Mr. Arvind Wadhera, Ms. Raluca Painter, Internal Market & Services DG

## Annex 1

**Description of the main issues:**

*1. Ratio of Directive on statutory audits and the Commission Decision 2010/485/EU*

Both, the Directive 2006/43/EC and the Commission Decision 2010/485/EU have been implemented to foster more effective and efficient cooperation and information sharing between financial regulators in the EU and with specific third countries that are deemed equivalent for audit purposes: "The global nature of corporate activity demands that audit regulators share information and cooperate across borders"[7]. Both pieces of legislation permit and facilitate the sharing of personal data in this context.

It is of paramount importance that the transfer of data between the European competent authorities and the PCAOB corresponds to the purpose of cooperation for the oversight of statutory audits: Personal data can be processed in this context only for the aforesaid purpose and according to the criteria expressed by the request for relevant documents (as specified under Directive 2006/43/EC).

The PCAOB approached several European audit regulators last year to transfer data to it under non-binding bilateral arrangements. Such arrangements include procedural documents containing provisions aimed to ensure privacy and/or data protection. Some Member States have already concluded or are in the process of developing such non-binding arrangements in particular by using article 26.2 of Directive 95/46 to adduce adequate safeguards, as previously mentioned in the Opinion WP 143.

There appears to be increasing pressure to conclude such bilateral non-binding arrangements due to, a.o., the fact that the auditing schedule (usually carried out every 3 years) has, since 2009, been postponed.

*2. Different approach in Member States vs. disclosure of personal data*

The potential result of Member States approaching this issue differently under existing national laws in Member States, rather than having an EU level approach, raises the concern that this could lead to Member States' oversight authorities and audit firms disclosing personal data inconsistently and result in "forum shopping" from US authorities because disclosure of personal data to third countries will occur under different terms and conditions with respect to data protection.

[7] Press release 10 January 2011 published on http://www.gti.org/Press-room/GT%20welcomes%20greater%20cooperation%20between%20audit%20regulators.asp

The different statutory requirements in Member States are, in the view of WP 29, likely to exacerbate this situation. Firstly, some countries[8] are resisting such an approach due to local legal obligations of professional secrecy and/or the protection of business secrets that apply to auditors; and secondly, the different application of Article 20 of Directive 95/46 amongst Member States, for example national requirements may include, but are not be limited to, specific conditions such as the use of public guidance by the DPA[9], privacy impact assessments or security audits. Some Member States may also require information prior to the transfer, prior notice/authorization of the NDPA, or even a formal opinion. The WP 29 does not dispute the capacity of the competent authorities of the Member States to take those decisions on the basis of their own assessment and national legislation. It merely expresses its concern about the consequences that a fragmented approach may entail.

**Analysis**

1. Positive elements regarding the initial harmonization efforts by DG MARKT and EGAOB in application of article 26.2. Directive 95/46/EC

The WP 29 has found several positive elements during its analysis of this issue. The Commission has already confirmed that the EU data protection legislation does indeed apply to these transfers[10] and that the privacy of the clients of statutory auditors and audit firms should be respected[11], i.e. the Commission Decision[12] states: *"Accordingly, where a transfer of audit working papers or other documents held by statutory auditors or audit firms to the competent authorities of Australia or the United States involves the disclosure of personal data, it should always be carried out in accordance with the provisions of Directive 95/46"*.

In addition, the EGAOB has encouraged a common approach via the development of a model MoU on the cooperation and the exchange of information related to the oversight of auditors. This document represents a template, which all the public oversight bodies of the Member States could collectively sign up to and/or use to negotiate bilateral agreements with the relevant third countries' competent authorities.

However, whilst this solution would offer more harmonization, Member States would remain free to choose a derogation such as article 26.1 (d) Directive 1995/46 - "important public interest grounds". For any application of article 26.1 (d) Directive 1995/46, the WP 29 recalls its Working Document WP 114[13]. The WP recommended that the use of derogations under article

[8] See for instance Belgium and France

[9] One bilateral agreement referred to public guidance of one NDPA. It is positive that public guidance of one NDPA is used. However, any technique of self-assessment should always be used with care as it requires specific legal advice and should take into account all differences of both legal systems.

[10] Page 3 points 1.1. in fine and 1.2. (4) of the Letter EC of 9 February 2009, published on http://ec.europa.eu/internal_market/auditing/docs/comment_letter_en.pdf .

[11] Recital 10 Directive 2006/43 *"It is important that statutory auditors and audit firms respect the privacy of their clients. They should therefore be bound by strict rules on confidentiality and professional secrecy which, however, should not impede proper enforcement of this Directive. Those confidentiality rules should also apply to any statutory auditor or audit firm which has ceased to be involved in a specific audit task."*

[12] Recital 5 Commission Decision of 1 September 2010.

[13] Working document of 25 November 2005 on a common interpretation of Article 26(1) of Directive 95/46

26.1 should be *"strictly interpreted"*[14] and that, although *"there will be cases where mass or repeated transfers can legitimately be carried out on the basis of Article 26(1)"*, when certain conditions are met, *"transfers of personal data which might be qualified as repeated (…) or structural should, where possible, and precisely because of these characteristics of importance, be carried out within a specific legal framework(…)."*[15]

2. Data Controllership

The WP 29 understands that, since the cooperation is based on Article 47(1) of Directive 2006/43 and Article 47(1) (b) expressly states that "the transfer takes place via the home competent authorities to the competent authorities of that third country and at their request"[16], the official point of cooperation and exchange of information for the PCAOB will be the European oversight bodies[17].

The WP 29 is of the opinion that article 47 (4) of Directive 2006/43 should only be used under the terms and conditions specified in that article.

It is likely that both audit firms and audit authorities could be considered as data controllers for their respective, different processing operations. The processing operations for European oversight bodies concern taking "responsibility for these issues in bilateral arrangements with public oversight bodies from third countries as required under Article 47 of the Statutory Audit Directive)"[18].

3. Scope of the data transfers (three elements)

The current data transfers consist of three elements: public audit reports, non-public audit working papers (supporting documentation) and inspection reports of authorities of the Member States – all of which contain personal data.

The WP 29 understands that the primary focus of personal data in the transfer will be: *"the names, and information relating the professional activities, of the individual persons* (auditors) *who were responsible for or participated in the audit engagements selected for review during an inspection or who play a significant role in the firm's management and quality control"*[19]. However, the WP 29 is concerned that whilst this is true for the publicly available audit reports, this will not be the case for the non-public audit working papers. The audit working papers are supporting documentation to the public audit reports, the content of which will often fall under national professional secrecy laws and may contain sensitive data related to individuals working for clients of audited companies (i.e. head of accounting dept. X, in branch Y, of company Z), as

[14] Page 2 of the working document WP 114. "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)."
[15] Page 9 § 4 of the working document WP 114
[16] See page 2 pt. 1.1. of the letter of the European Commission of 9 February 2009 to the PCAOB, published at http://ec.europa.eu/internal_market/auditing/docs/comment_letter_en.pdf and Decision 2010/485/EU, 1/9/2010,article 2(5)
[17] See page 2 pt. 1.1. of the letter of the European Commission of 9 February 2009 to the PCAOB, published at http://ec.europa.eu/internal_market/auditing/docs/comment_letter_en.pdf
[18] Directive 2006/43
[19] Wording found in one draft PCAOB of 10 May 2011 between the PCAOB and one Member State.

well as (potentially) issues of illegal, suspicious or fraudulent activities in relation to the individual's functions within the audited company. Similar concerns exist with regard to inspection reports.

Therefore the privacy and data protection of auditors (natural persons) should not be the only consideration but also that of individuals working for their clients who appear in the audit reports or related documents that support the audit findings. Restricting data protection to the "top level" (i.e. just the auditors/natural persons) is inadequate, especially because the audit working papers and inspection reports are more likely to contain sensitive personal data.

4. Nature of the data transfers

The transfers appear to be repetitive in nature[20] (periodic cooperation) and occur within a structured mechanism (for instance a bilateral arrangement between PCAOB and EU authorities). There is currently no indication that the scope of the transfer would be large or in bulk form – both of which, in other contexts, have been criticized by the WP 29 previously[21].

5. Legitimacy

Currently, the legitimacy of the transfers to the PCAOB remains entirely subject to the conditions of the national legislation implementing the provisions of the Directive 95/46[22], by either applying the derogation under articles 26.1 (d) or 26.2 of Directive 95/46 (see above). However, moving forward, the WP 29 urges the Commission to find legitimacy in a harmonized regulatory basis at an EU level rather than in different national laws and different bilateral approaches under Directives 1995/46 and 2006/43.

6. Necessity of cooperation vs necessity of data transfers

The necessity of cooperation was worded as follows in recital 28 of Directive 2006/43: ""*The complexity of international group audits requires good cooperation between the competent authorities of Member States and those of third countries. Member States should therefore ensure that competent authorities of third countries can have access to audit working papers and other documents through the national competent authorities. In order to protect the rights of the parties concerned and at the same time facilitate access to those papers and documents, Member States should be allowed to grant direct access to the competent authorities of third countries, subject to the agreement of the national competent authority.(…).*"

The WP 29 does not question the need for cooperation between competent authorities of Member States and those of third countries, but the WP 29 must highlight the difference between the desire to enhance cooperation and the necessity of data transfers as a factor to achieving this goal.

[20] Oversight by the EU and US oversight bodies is carried out on a regular basis (in the US every three years).
[21] See the data transfers via black box construction under the TFTP2 Agreement.
[22] See page 3 point 2 of Opinion WP38 01/2001 published on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp38en.pdf

The WP 29 understands the willingness of all parties (i.e. auditors and inspections by authorities of EU and third countries) to achieve "mutual reliance"[23], i.e. that cooperation between audit authorities should be possible without any requirement of data disclosure once the equivalence of certain third country public oversight, quality assurance, investigation and penalty systems for auditors and audit entities has been confirmed. However, mutual reliance implies the absence of necessity for the data transfers and therefore lacks the best data protection possible which should be the first priority of all EU audit authorities.

7. Definition of purposes / purpose limitation / safeguards

Once necessity of the data transfers has been established, all parties must apply the principles of data minimization and proportionality. This means ensuring that transfers of personal data are the exception and not the rule. For such exceptional transfers of personal data, it should be clear what information are necessary, and whether personal data needs to be disclosed, as well as having a clear legal basis and specific guarantees in place.

The WP 29 can only assume that not all personal data contained in non-public working papers and inspection reports to be transferred will be relevant in relation to requests of cooperation and therefore the Commission should clarify with the PCAOB to what extent they find the information necessary. From the information available to the WP 29, it appears that the PCAOB reserves the right to request all *"information and/or if requested, reviewing audit work papers and other documents, interviewing firm personnel,…"*.[24]

Furthermore it is also unclear whether the disclosure is made subject to a clear legal basis and specific requests that indicate a clear, legitimate purpose (article 8 ECHR). Again, disclosure that is limited to what is "strictly necessary and relevant for the purposes of the ad hoc investigation"[25] should be respected.

Recital 2 of the Decision makes the purpose of the transfers clear: "any such transfer by the competent authorities of Member States should be made solely for the purpose of the exercise of the competences of public oversight, external quality assurance and investigations of auditors and audit firms by the competent authorities of the third country concerned". However after reviewing the existing bilateral statements the legitimate purposes for both primary and potential onward data transfers (article 6.1 (b) Directive 95/46) have not been made explicit. The WP 29, therefore, encourages the use of the relevant, specific paragraphs such as in the EGAOB model MoU that refers to specific purposes such as "improve the quality of auditing" and "to protect investors and to help strengthen public trust in the auditors report and increase investor confidence in their respective capital markets". When creating the MoUs specific wording should be used and not vague statements that could be left open to the discretionary

[23] See a.o. article 34 Directive 2006/43 (within the EU), See recital 17 and 18 if Commission Decision of 1 September 2010 on the adequacy of the competent authorities of Australia and the United States pursuant to Directive 2006/43 of the European Parliament and of the Council; recital 14 of the Commission Decision of 5 February 2010 on the adequacy of the competent authorities of certain third countries pursuant to Directive 2006/43 of the European Parliament and of the Council (Canada, Japan, Switzerland), recital 3 and 6 of Commission Decision of 19 January 2011 on the equivalence of certain third country public oversight, quality assurance, investigation and penalty systems for auditors and audit entities and a transitional period for audit activities of certain third country auditors and audit entities in the European Union

[24] See article III. A.2. Cooperation of the Statement of Protocol between the PCAOB and the POB of 10 January 2011.

[25] See page 4, point ii of Opinion WP 143.

interpretation of one of the parties[26] and/or which may even be beyond the control of the disclosing parties[27].

Clear purpose limitation wording should impose binding obligations on all parties to refrain from uses that would conflict with national data protection or secrecy obligations of the disclosing authority and/or legislation that protects business secrets. If MoUs lack clear obligations to refrain from such use or if such obligations are not binding on the receiving competent authority, this raises concerns about compliance if possible recipients on foreign soil[28] are taken into account. This concern should at least be addressed with mechanisms such as the consent of the disclosing authority, as seen in other files[29].

Disclosing authorities should provide procedural "filtering" guarantees (push disclosure, anonymization…) and accountability in case of exceptional joint inspection teams

Most arrangements appear to contain "prior notice" and "prior consent" requirements[30] that appear to give some protection to the disclosing supervisory body and the data subjects in their respective countries from the use of information for other purposes than initially defined in MoUs. However, unless combined with other guarantees, these techniques may only offer limited protection against function creep (above) and insufficient respect for the proportionality requirement (necessity and data minimization). Indeed, it will not always be in the power of the disclosing authority to prevent, nor consent to, disclosure of information that would in itself constitute an illegal act in the country of origin (i.e. sending the full list of employees). In other words, the risk exists that the "prior notice" and "prior consent" requirements are insufficient safeguards.

The WP 29 suggests adding additional procedural guarantees that can work as filtering mechanisms at the level of disclosing authorities, including in the exceptional cases of joint inspections.

"Push" disclosure by disclosing authorities with data protection safeguards should be the rule instead of simply handing over personal data without specific safeguards. However, from its analysis of existing bilateral arrangements, it would rather appear that the PCAOB could make

[26] Such as "the personal data exchanged between the competent authorities shall be used by the receiving authority solely for the purposes of implementing this Protocol".

[27] Such as general references used in accordance with the national law of the country of the receiving party. See clauses such as "personal data may be processed by the PCAOB only for the purposes permitted or required by the Sarbanes-Oxley Act of 2002 (the "Sarbanes-Oxley Act") and any rules or regulations promulgated there under, that is, for the purposes of oversight, inspections and investigations of registered auditors or audit firms and their associated persons subject to the regulatory jurisdiction of the PCAOB and(…)".

[28] The PCAOB Data Protection Practices and Policies of May 2006 mentions at its page 6 "under the Sarbanes-Oxley Act the Board may share information with the SEC (The security exchanges commission oversees the PCAOB) as well as certain other federal and state authorities when its determines in its discretion that it is necessary to accomplish the purposes of the Act or to protect investors." (For instance, the US Attorney General and US State Attorneys may become possible recipients of the information.)

[29] See the mechanism of FIU consent mentioned in the annex to Opinion WP 186.

[30] See wording such as "The use of personal data, for further purposes by the Authorities or public bodies of the Party which received the information shall only be authorized after prior express and written approval of the authority of the Party which transmitted the information in accordance with the legislation of that Party which transmitted the information. Such use shall then be subject to any conditions established by that authority."

"broad requests"[31] to receive any data set (see point 2) without offering specific, written or narrowly tailored requests (i.e. making requests by telephone). This could be interpreted as "bulk" transfers. The WP 29 has recommended in other contexts[32] the need to establish different "push" / "pull" modalities in relation to transfers. Whilst in this scenario there is no risk of a direct "pull" scenario (i.e. no direct database access) between EU and foreign authorities, it is still unclear how EU oversight bodies and auditors are approached directly by foreign authorities for this information. It is also unclear if the PCAOB requires all publicly available reports initially, which would then trigger further requests for non publically available reports, or if the PCAOB requires only a sample of non-publically available reports, or even if the PCAOB requires 100% of all three elements of audits reports over the three year period set out in the Commission Decision. Furthermore, it is unclear to the WP 29 whether there is a consolidation of data by auditors at global level, as witnessed in the area of AML/CFT processing operations.

In addition, disclosing authorities should use other data blocking techniques such as anonymization[33] of submitted documents.

In the exceptional[34] case of joint inspection teams, accountability mechanisms should be provided, including but not limited to the signing of non disclosure agreements vis-à-vis the disclosing authority by all members of joint inspection teams. The modalities of joint inspection teams should also be clarified, in accordance with national data protection law of that Member State that may require specific measures under article 20 Directive 95/46/EC.

8. Restrictions to rights of access, rectification, objection or deletion

In the existing bilateral arrangements with the PCAOB the WP 29 found evidence of restrictions to the rights of access, rectification, objection or deletion . However other agreements would seem to award more weight to these rights as well as to the multiple conditions required for such restrictions on public interest grounds.

To the extent that these exceptions and restrictions are indeed based on differences of national law in the Member States as foreseen by article 13 of Directive 95/46, the WP 29 recalls its previous comment of a strict, limited and case-by-case application of these exceptions (in the short term), as well as (in the long term) the need for a harmonized approach via a durable, legally sound European solution.

9. Redress and control mechanisms and independent supervision on foreign soil extraction

Not all the existing bilateral transfer arrangements offer a clear instrument for redress or accountability. Different approaches in the Member States to article 20 of Directive 95/46 may

[31] Vague requests that contain no specific motivation, scope or necessity.
[32] See the PNR opinions.
[33] for instance by blackening personal data from disclosed documents
[34] See article 2(6) of the Commission Decision 2010/485/EU of 1 September 2010 : *"Member States may agree to joint inspections only where necessary (…) (and) under the leadership of the competent authority of the Member State concerned."* Hence, joint inspection teams should remain the exception, especially in cases where the only basis is a non binding agreement. One should take into account the wide opportunity to collect information n foreseen in such non binding agreements (for instance under article III. B. 9 of the statement of protocol between POB and PCAOB of January 2011) , combined with the risks that are linked to any lack of binding commitment to respect basic rules of confidentiality

have a direct impact on the assessment of what is considered public interest grounds for the transfer of personal data, as defined in the applicable national law[35]. Therefore a harmonized approach would be preferable.

10. Adequate data protection requirement: interpretation of "adequate data protection", legal basis and required safeguards

10.1 Double meaning of "adequate data protection" in the EU Directives

It appears that the term "adequacy" continues to add confusion in relation to its use in Directive 2006/43 and the different commission Decisions[36].

The WP 29 has already highlighted in its previous opinion the difference between the adequacy test in the areas of audit supervision and data protection[37]. The double use of the adequacy requirement in Directives 2006/43 and 95/46 remains a possible cause for misunderstanding[38]. Even though article 47 of Directive 2006/43 (e) and the Commission Decision clearly refer to chapter IV (articles 25 and 26) of Directive 95/46, there is still confusion on the exact conditions that should accompany any international data transfer.

When drafting future "audit adequacy decisions" or other audit legislation, the Commission should make clear the difference of adequacy under both regimes.

10.2 Consequences of the double legal basis for international transfers under Directive 95/46

The approach of the Commission Decision of 1 September 2010 seems to focus mainly on article 26.2 Directive 1995/46. Indeed, recital 5 of the Commission Decision of 1 September 2010 requires "in particular" (…) "binding agreements" as an appropriate safeguard.

The possibility for Member States to choose between either articles 26.1 (d) or 26.2 Directive 1995/46/EC should not be forgotten, as well as the specific questions that are raised by the choice for article 26.1 (d)[39] .

The specific questions appear to be mainly

* if the data controller decides to choose important public interest grounds as the legal basis to transfer personal data, it should be recognized that this derogation only applies to the transfer of personal data, and that all the data protection principles remain in force. The WP 29 has previously provided guidance in document WP 114[40] and referred to a set of 'core' data protection 'content' principles and 'procedural/enforcement' requirements that are seen as a

[35] See page 4 point i of Opinion WP 143 ("It is the responsibility of the national oversight authority (competent for the audit) performing the transfer to decide on whether there is a substantial public interest, using a case-bycase approach in the light of the relevant domestic legislation and taking into account, where appropriate, an opinion by the national DP authority."
[36] A.o. decision 2010/485/EU
[37] See Opinion WP 143 page 3 (last bullet point).
[38] See article 25.2 DP Directive 1995/46 vs. article 47(1) € Directive 2006/43 and recital 6 Commission Decision 2010.
[39] See working document WP 14 of 25 November 2005 on a common interpretation of Article 26(1) of Directive 95/46
[40] See working document WP 114 of 25 November 2005 on a common interpretation of Article 26(1) of Directive 95/46

minimum to ensure "adequate protection". The WP 29 has commented the (lack of) presence or quality of these elements in different opinions, such as in negotiations and agreements with the US.

* can the receiving authority define unilaterally the meaning of public interest grounds, for instance by referring to its national law in the cooperation agreement. In this matter, the WP 29 recalls the conclusion of its opinion WP 143, stating that article 26 (1) (d) of Directive 95/46 *"should be interpreted restrictively by having regard to the substantial public interest served by the transfer (as vested either in the individual Member State or in the EU) and by ensuring that only relevant and necessary personal data are transferred for the sake of such substantial public interest."*

The WP 29 also believes that Article 47 of the Directive 2006/43 could provide a legal basis to share auditing information, provided that the legal requirements in both article 47 Directive 2006/43 and articles 25 and 26 Directive 95/46/EC[41] are met.

Previously, the Commission[42] found the use of the Safe Harbor scheme to be non-applicable to PCAOB transfers.

In its previous opinions on the application of article 26.2 of Directive 95/46 on statutory audits[43], the WP 29 expressed its confidence in the flexibility of the application of the standard contractual clauses in this context in order to provide adequate data protection safeguards. However, the use of contractual clause wording in the process of negotiating and drafting bilateral agreements is not without difficulty. Also, it should be reminded that this approach remains limited to the application of article 26.2 Directive 1995/46.

For the sake of clarity, the WP 29 repeats that such harmonized approach under article 26.2 Directive 1995/46 "does not rule out the need for the national competent authority to check – in the light of domestic legislation – whether the preconditions to allow the disclosure of data to the third party competent authority are fulfilled."[44]

---

[41] See recital 29 Directive 2006/43 : *"Disclosure of information as referred to in Articles 36 and 47 should be in accordance with the rules on the transfer of personal data to third countries as laid down in Directive 95/46 (…)"*
Consequently, the European Commission's equivalence decisions such as the Commission Decision of 1 September 2010 2010/485/EU may be confused with but cannot replace the requirement of adequate data protection in the meaning of article 25.2 DP Directive 1995/46. The WP 29 recalls its recommendation n° 40 attached to Opinion WP186 of 13 June 2011, opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing : "*Adequacy findings (…) should always contain a rigorous process that contains a comparison of the level of protection provided in the specific country with EU privacy and data protection standards* by DPAs and/or the European Commission as described under articles 25.2, 25.3 and 25.6 of Directive 95/46.*"*

[42] With regard to transfers of information to the PCAOB, the European Commission previously stated that *"Transfers to US organizations (public or private) that are not "Safe Harbor" members do not ensure this adequate level of protection. As PCAOB is not part of the "Safe Harbor" scheme, a national data protection authority in a Member State of the European Union can only authorise a transfer on the basis of a transfer agreement concluded under Article 26 (2) of the Directive 95/46. Such agreement should contain special safeguards which are put in place with respect to the protection of the privacy and fundamental rights and freedom of individuals and as regards the exercise of the corresponding rights."* (Page 3 point 1.2. (4) of the Commission Letter of 9 February 2009, published on http://ec.europa.eu/internal_market/auditing/docs/comment_letter_en.pdf ) .

[43] See pages 4-5 of WP 143 of 23 November 2007, and also WP 114 of 15 November 2005, WP 66 of 24 October 2002 and WP 128 of 22 November 2006.

[44] See page 5 § 2 Opinion WP 143.

The WP 29 reminds also that when compliance with Chapter IV of Directive 95/46/EC is ensured by recourse to Article 26.1 (d), since it derogates from the general regime, it should be interpreted strictly and that, even in using it, introducing additional safeguards aimed to ensure that the rights and freedoms of the data subjects are upheld should be strongly recommended.

In the case where Article 26.1 (d) would be used as a legal basis for the transfer, it would mean, (if a substantial public interest was found) derogation of a data controller from his duty to assess the level of protection afforded by the third country, or obtain prior authorization of the transfer where applicable;.
The WP29 recalls document WP 114 which not only outlines the above allowances but states "the interpretation of the Article 26(1) must be necessarily strict"[45]. The strict interpretation of the article is to ensure that data controllers do not make the exemptions their first choice, and can only be used when … for the most part [it] concern[s] cases were 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"[46].

In this regard, also in order to avoid the aforesaid problem of "forum shopping", it would be advisable to foresee a harmonized procedure in case of controls - on the same undertaking - by competent oversight authorities in different Member States. Harmonization efforts should also reinforce the data minimization and mutual reliance principles by requiring written, specific and justified requests that mention the purpose and necessity of such documents for the case under review.

**Conclusion**

The WP 29 reaffirms its willingness to engage in close cooperation with the Commission and the EGAOB to resolve the issues identified above. However, in the short term WP29 advises to follow the recommendations set out below, and, in the long term, work together to encourage a more EU harmonized approach.

The WP 29 will reassess its position based on the outcome of this approach, and may prepare one or more additional opinions and/or letters in this field if this is deemed necessary.

[45] Opinion 114, adopted November 2005, page 7, paragraph 6
[46] Opinion 114 Page 7 para 3

## Annex 2

**Additional 12 recommendations**[47] that address data protection compliance issues in agreements concluded by disclosing authorities

Rec. 1. Any agreement with the PCAOB should contain a clear applicable legal clause which, at the very least, acknowledges the applicability of EU and national data protection laws, and professional secrecy legal obligations that apply to disclosing authorities , oversight bodies, audit companies and companies established in the Member States.

Rec. 2. The WP 29 refers to its previous opinions[48] and recommends the EGAOB and the Commission to carefully define the data protection safeguards in relation to the application of article 26.1 (d) Directive 95/46 ("important public interest grounds", if this legal basis is chosen instead of article 26.2 Directive 95/46). The WP 29 also encourages the EGAOB and the Commission to negotiate a more harmonized and consistent procedure in case of controls with the PCAOB that provides filtering techniques and accountability mechanisms in case of any exceptional disclosure of information by the competent authorities in different Member States. Referring to WP29's previous opinions[49] and taking into account the content of existing agreements with the US in other sectors (PNR[50], TFTP2[51]) and the expected overarching agreement between the US and the EU should help to achieve this consistency.

Rec. 3 Given that Directive 95/46 applies to all transfers of all personal data to a third country's competent authorities, such as the PCAOB, appropriate attention should be given to the different necessity and conditions that may be present for transfers of personal data at different levels,( personal data in public audit reports, in non-public working documents and in audit inspection reports).

Rec. 4 In cases where a transfer of personal data is considered to be sent to a recipient without adequate data protection in the meaning of Directive 95/46, the WP 29 encourages competent authorities to enquire with their in-house legal counsels and/or NDPAs on the current requirements and best practices that are available under the national data protection law before the adoption of any agreement and before any disclosure to third countries.

Rec. 5 Appropriate attention should be paid to a (1) clear definition of the purposes of cooperation clauses as well as (2) a purpose limitation principle clause and (3) safeguards which also apply in cases of article 13 (1) Directive 95/46 (article 8 ECHR).

[47] See previous guidelines attached to Opinion WP 143.

[49] See WP 12 "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", adopted on 24 July 1998."

[50] Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), OJ, L 204/18 of 4 August 2007.

[51] Agreement of 28 June 2010 between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195/13 of 27 July 2010

Rec. 6. The WP 29 recommends to confirm the principle of mutual reliance. This implies that transfers of personal data should always remain exceptional (judged on a case by case basis), and that any "push" (disclosure) scenario should contain specific data protection guarantees. It should always be made clear what, if any, personal data is necessary to fulfill the request (and for what purpose). Handing over personal data upon the basis of open, general requests by foreign authorities should never occur.

Rec. 7 In addition to the "prior notice" and "prior consent" requirements in existing agreements, the WP 29 recalls its Opinion WP 143 of 23 November 2007[52]. Disclosing competent authorities should have specific data protection guarantees such as filtering or anonymisation mechanisms, including accountability as a condition for joint inspection teams, in accordance with national data protection law of that Member State.

Rec. 8 In the long term (i.e. after the expiry date of the Audit adequacy Decision on 31 July 2013), the WP 29 also supports the similar request by the European Parliament to negotiate a harmonized approach via a durable, legally sound European solution to the issue of data transfers[53] within the EU as well as to third countries.

Rec. 9 In case of application of the legal ground "important public interest" to justify transfers to the PCAOB (article 26.1 (d) Directive 1995), the WP 29 recalls its recommendations in working document WP 114. In application of these previous recommendations, such derogations under article 26.1 Directive 95/46 should be interpreted strictly. Also, repeated or structural transfers vis-à-vis the PCAOB should be carried out within a specific legal framework (i.e. preferably under a harmonized EU legal framework or binding agreements). Also, the need for more consistency with existing international agreements in other sectors[54] and the expected "umbrella" agreement between the US and the EU should be guarded.

Rec. 10. In case of application of the "adequate safeguards" legal ground under article 26.2 Directive 1995/46 for transfers to the PCAOB, the WP 29 recommends that it should compare the content of the contractual clauses, the draft European model agreement of the EGAOB and the different PCAOB model agreements, in order to draft an agreement resulting in an updated EU model agreement in the mid-long term, in close cooperation between the EGAOB and the Commission.

[52] See point II. Page 2 of this opinion that refers to the conditions for data transfers contained in article 47 of Directive 2006/43.
[53] See page 1 of EC Communication COM(2011) 429 final, published on http://ec.europa.eu/home-affairs/news/intro/docs/110713/1_EN_ACT_part1_v15.pdf.
[54] PNR, TFTP2, …

Rec. 11. For national audit supervisors that are currently urged to enter into immediate negotiations and sign arrangements with the PCAOB, the WP 29 encourages as "interim solution" the use of the model MoU of the EGAOB[55], and would welcome that the current negotiations to conclude bilateral arrangements with the PCAOB also take into account the acquired principles, rights[56] and guarantees that were accepted in existing agreements for other sectors[57] and the revision process of Directive 2006/43[58].

Rec. 12. Audit companies should have segmented data consolidation of audit reports and working documents (data storage in zones with adequate data protection in the meaning of Directive 95/46)[59] rather than to proceed with global data consolidation or data consolidation in zones without adequate data protection.

[55] Memorandum of Understanding on the cooperation and the exchange of information related to the oversight of auditors

[56] Some of these elements include but are not limited to (indirect) rights of access and rectification, accountability and redress mechanisms, powers of investigation of complaints by data protection authorities, reporting of independent supervisory authorities to national and European parliament,…

[57] PNR, TFTP2, …

[58] In this context, the inclusion of termination clauses in the MOUs or protocols can be recommended.

[59] See also recommendation n° 25 attached to the Opinion 14/2011.