

Chapter 4

Paragraph 4.28

State DPAs in Germany have questioned the legal sufficiency of the standard contractual clauses. German data protection law implements a two-step approach for use of the clauses: in the first step, an assessment is made of whether or not there is a legal basis for processing personal data under German data protection law, in particular under § 4 or § 28 of the German Federal Data Protection Act. The use of standard contractual clauses may then be considered in a second step in order to assess whether or not ‘adequate safeguards’ are ensured according to § 4b and § 4c para. 2 of the Act (which implement Articles 25 and 26 of Directive 95/46/EC).

In a paper adopted by the *Arbeitsgruppe ‘Internationaler Datenverkehr’* of the group of German data protection authorities (a subgroup meeting on international data transfers of the conference of German federal and state data protection authorities or *Düsseldorfer Kreis*) on 12-13 February 2007, it is stated that the alternative standard contractual clauses of 2004 are not suitable for the transfer of employee data and may need to be expanded by additional clauses, since the liability and informational obligations are ‘limited’.¹ This follows a paper dated 6 June 2006 prepared by the DPA of the federal state of Hessen in preparation for a meeting in Berlin of the *Arbeitsgruppe* which raises various questions about the adequacy of the alternative standard contractual clauses. In particular, questions are raised about the lack of joint and several liability (Clause III.a), the provision concerning the data importer’s duty to give information about processing to data subjects (Clause I.d), and the assertion of rights primarily against the data importer (Clause II.b) (see pages 4-5). The paper asks if these provisions are ‘acceptable’ (‘Sind diese Regelungen...akzeptabel?’). The paper then goes on to question the adequacy of Clause II.d, and para. 7 of Annex A.

The General Directive does not give a clear indication of the boundary between the two steps of the legal analysis that must be undertaken when determining the legality of an international data transfer. However, such a boundary can be defined by examining the purpose of the two steps. The purpose of step one is to ensure that the initial processing of personal data is legal under applicable national law, whereas the purpose of step two is to ensure that adequate protection or adequate safeguards will apply to processing of the data once they have been transferred outside the EU. Thus, for example, it is entirely legitimate for national law to require the conclusion of an agreement with the works council before employee data can be transferred under the standard clauses, since this requirement may derive from national employment law and is often required even for transfers of personal data within the EU, i.e., it is not directed solely at ensuring an ‘adequate level of protection’ for data transfers outside the EU. However, any criticism of the level of protection of specific provisions of the standard contractual clauses must be found to involve step two, since the clauses are

¹ Abgestimmte Positionen der Aufsichtsbehörden in der AG ‘Internationaler Datenverkehr’ am 12./13. Februar 2007, p. 2.

designed to provide adequate safeguards for the international transfer of personal data.²

The German DPAs are in effect attempting to ‘repackage’ concerns that actually relate to the level of protection under step two as falling within their discretion to ensure that there is a legal basis for processing under step one; for example, in the minutes of the Berlin meeting referred to above, it is stated that ‘in examining the first step (‘protectable interest of the data subject’) data export agreements which are insufficient under German law may be taken into account’.³ The criticisms they make about the standard clauses clearly concern the substance of the protections included in them, rather than the initial legality of processing, and thus fall within step two, which has been settled once and for all by the Commission decisions. For example, any criticism that the alternative clauses results in a ‘lowering of the level of data protection’ (*Absenkung des Datenschutz-niveaus*) as in the article by the Berlin DPA quoted above is clearly calling into question the Commission decision approving the clauses as offering ‘adequate protection’. While the DPAs state in the minutes of the Berlin meeting that ‘the first step (material permissibility under national law) may not be evaded by signature of the alternative standard contractual clauses in the second step’,⁴ the reverse is also true: the legal effect of the Commission’s decisions approving the standard contractual clauses as providing ‘adequate protection’ may not be evaded by deeming questions related to the adequacy of protection (step two) to fall within the DPAs’ discretion to determine compliance with national law (step one). While the DPAs do have the discretion under national law to determine the conditions for satisfying step one, such discretion is not unlimited, and must be subordinate to conflicting rules under EU law.

Under Article 249 para. 4 of the EC Treaty, any Commission decision is binding upon those to whom it is addressed, and the Commission decisions on the standard contractual clauses are addressed to the Member States (see Article 7 of the 1001/497 Decision, and Article 3 of Decision 2004/915). A decision which has been addressed to all Member States constitutes a legislative act,⁵ and is binding on all institutions of the Member State concerned, including the judiciary. Accordingly, Member States are under a duty by virtue of the primacy of Community law to refrain from applying any

² See Article 26(2) of Directive 95/46/EC.

³ Page 5: ‘Bei der Prüfung der 1. Stufe (,schutzwürdige Interessen des Betroffenen’) können (nach deutschem Recht unzureichende) Vereinbarungen über den Datenexport bereits berücksichtigt werden’.

⁴ Page 6: ‘Die 1. Stufe (materielle Zulässigkeit nach nationalem Recht/BDSG) könne nicht durch den Abschluss der (Alt.) StV auf der 2. Stufe umgegangen werden’.

⁵ See, e.g. Council Decision 98/415/EC of 29 June 1998 on the consultation of the European Central Bank by the national authorities on draft legislative provisions, [1998] O.J. L 189/42. Regarding decisions addressed to the Member States, see Mager, ‘Die staatterichtete Entscheidung als supranationale Handlungsform’ (2001) EuR 661-681.

national provisions which would be likely to hinder the implementation of a Commission decision.⁶

Based on case law concerning the correct implementation of directives, national authorities are under a duty to refrain from applying national provisions which conflict with the provisions of a directive.⁷ Moreover, all the authorities of a Member State must take, according to their respective powers, all the general and particular measures necessary to ensure that the result sought by the Directive in question is achieved.⁸ In this case, the result sought by a Commission decision under Article 26(4) of Directive 95/46/EC is to provide a standardized way of transferring personal data outside the EU, and this result is frustrated if a Member State DPA regards the adequacy of a data transfer method standardized by a Commission decision as falling within its national competence.

Apart from the substantive data protection issues involved, the way that the German DPAs are raising these issues holds the potential to severely damage the utility of the standard contractual clauses. If the DPAs believe that the clauses do not offer 'adequate safeguards', then the correct course of action is for them to discuss this issue within the Article 29 Working Party and have the Working Party attempt to convince the Commission to modify its decision, or, failing this, to bring suit against the Commission under Article 230 of the EC Treaty, rather than each national or local DPA taking unilateral action on a national level. If each DPA were to take similar action on its own, then there would soon be at least 27 different sets of additional national requirements to be fulfilled when using the standard contractual clauses, and they would become useless. In fact, this multiplicity of national requirements for approval of contractual clauses, which was the case before the standard clauses were approved, was precisely the situation that the standard contractual clauses were supposed to remedy.

This is not just a German issue: if other Member State DPAs raise additional challenges to the adequacy of the alternative standard contractual clauses, then this will effectively make the Commission decisions approving them useless.

Paragraph 4.61

A company's safe harbor certification is valid for one year from the date that it is entered into the safe harbor list by the US Department of Commerce.

Paragraph 4.66

In June 2007, the European Commission announced that it had rejected a complaint raised by a Greek legislator that the transfer of personal data of the employees of the

⁶ ECJ, Case 249/85 *Albako* [1987] E.C.R. 2345, para. 17.

⁷ ECJ, Case 103/88 *Fratelli Costanzo* [1989] E.C.R. 1839, para. 33.

⁸ ECJ, Case C-72/95 *Kraaijeveld* [1996] E.C.R. I-5403, para. 61; ECJ, Case C-435/97 *World Wildlife Fund* [1999] E.C.R. I-5613, para. 70.

Greek subsidiary of the US company Abbott Laboratories violated EU data protection law. The Commission stated that Abbott's safe harbor membership meant that the transfer of the data to its headquarters in the US was not in breach of EU law.

Paragraph 4.109

In its opinion in the SWIFT affair, the Article 29 Working Party found that the transfer of personal data in the SWIFT database could not be justified under Article 26(1)(b) of the General Directive as being necessary for the performance of a contract between the data controller and a third party, without explaining in detail why this was so.⁹

Paragraph 4.115

In its opinion in the SWIFT affair, the Article 29 Working Party found that the transfer of personal data in the SWIFT database could not be justified under Article 26(1)(d) of the General Directive as being necessary or required on important public interest grounds, or for the establishment, exercise or defence of legal claims, since the SWIFT database could have been located in a country that had been found to offer an 'adequate level of data protection' (such as Argentina or Canada) rather than in the US, and the public interest involved was not that of an EU Member State.¹⁰

Paragraph 4.124

Germany: On 1 June 2007, the DPA of the German federal state of Hessen approved the BCRs of Merck.¹¹ The BCRs are wide-ranging and cover data of employees, business partners, customers, and suppliers, as well as clinical trial data.

UK: On 9 May 2007, the UK Information Commissioner approved the BCRs of Philips, which cover both employee and customer data.¹²

Paragraph 4.127

⁹ Article 29 Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (WP 128, 22 November 2006) 24.

¹⁰ Ibid.

¹¹ See the DPA's press release of 12 June 2007 (in German only) at http://www.rp-darmstadt.hessen.de/irj/RPDA_Internet?rid=HMdI_15/RPDA_Internet/nav/1e3/1e3605fe-78c2-9011-1010-43765bee5c94,ec40fe7f-dad1-311d-5ce7-b44e9169fccd,,11111111-2222-3333-4444-100000005002%26_ic_uCon=ec40fe7f-dad1-311d-5ce7-b44e9169fccd%26shownav=false.htm&uid=1e3605fe-78c2-9011-1010-43765bee5c94&shownav=false.

¹² See the Information Commissioner's press release at http://www.ico.gov.uk/upload/documents/pressreleases/2007/philips_authorized_by_ico_to_transfer_personal_information....pdf.

On 10 January 2007, the Article 29 Working Party adopted a recommendation for a standard application for approval of BCRs, which is based heavily on the ICC submission and adopts the majority of its text verbatim, with some important additions and deletions.¹³

¹³ Article 29 Working Party, 'Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data' (WP 133, 10 January 2007).