Berlin DPA supervises German Railway and Citibank TBDF contract

What happened when Citibank's joint credit card/season ticket venture with German Railways led to public demands for application of Germany's strict data protection law to their personal data transferred to and processed in the USA? Dr Alexander Dix, the Berlin Deputy Data Protection Commissioner, explains. The parties wanted a legal result which would satisfy not only current German law but also the EU Data Protection Directive's rules on transferring personal data to a country without adequate regulation, which would apply when the Directive is implemented in October 1998.

The German Federal Railway used to be a state-owned public monopoly. In 1994 it was privatised and became a public corporation, *the German Railway (Deutsche Bahn AG)*. The majority of its stocks is owned by the Federal Republic. The corporation still has, by and large, a monopoly in the German railway sector.

The problem began when the German Railway started to offer a discount system based on a plastic card, the RailwayCard (BahnCard). Holders of this card were entitled to certain considerable discounts when travelling by train in Germany. This card soon became very popular especially with commuters and old age pensioners. The card was equipped with neither a magnetic strip nor with a chip. The RailwayCard had to be applied for at train stations and was produced by a private German company, Bertelsmann.

"The better RailwayCard"

In November 1994, German Railway decided to co-operate with the German subsidiary of Citibank, one of the largest internationally operating banks. The two companies concluded a co-branding agreement which provided for the issuing of the RailwayCard with a payment function. All RailwayCards became VISA credit cards at no additional cost for the customer. The same applied also to old RailwayCards which were to be renewed on an annual basis. In addition, the RailwayCard carried the holder's photograph.

The RailwayCards, as well as the normal VISA cards issued to German Citibank customers as from July 1, 1995, were produced in the United States; more precisely in data centres run by Citibank subsidiaries in South Dakota and Nevada.

As soon as the first German train passengers wanted to renew their RailwayCard or to apply for a new one in July 1995, they were told that they had to accept the RailwayCard with the credit card function (advertised by German Railway and Citibank as "the better RailwayCard"). This applied even if they did not want a credit card at all, perhaps because they already had one.

Complaints and fears of data misuse

This railway/credit card led to numerous complaints and negative reports in the media about the whole co-branding deal which was said to be the biggest credit card agreement in Germany so far. It was widely believed in Germany that the German Railway monopoly had sold the data of its existing RailwayCard customers, and of all potential customers, to a big US-based bank which was very likely to use this data in the direct marketing business, and not simply for the individuals' own purposes.

The local German data protection supervisory authorities criticised a number of points in the application form issued by German Railway and Citibank, especially the fact that personal data on creditworthiness was collected from people who simply wanted to get on a train regularly.

Backtrack to the "pure" RailwayCard

Very soon - after strong public protests by consumer groups and data protection authorities - the Railway and Citibank had to re-negotiate the co-branding agreement to extend it to the production of the old-style RailwayCard without the credit card function and to offer it to customers as an option. It was called the "pure" RailwayCard (BahnCard pur). From the approximately 3,054,000 RailwayCards that had been issued to German customers by the middle of July 1996, the vast majority of cards were of this type, i.e. without the payment function. However, Citibank is now trying to increase the sales of the combined Railway VISA card.

Berlin Commissioner's view

On 1st August 1995, the Berlin Data Protection Commissioner took over jurisdiction for the German Railway. Discussions between the Berlin Data Protection Commissioner, the German Railway and Citibank made it clear that the German Railway, as the primary collector of the passengers' personal data, should not be allowed to outsource the whole issue of data protection in relation to the RailwayCard, especially in view of the fact that this outsourcing exercise led to a massive transborder data flow into a non-EU country, the USA.

Although the time limit to adapt national legislation to the Data Protection Directive (95/46/EC) expires only in October 1998, and Germany has not yet adapted its Federal Data Protection Act to the Directive, the Berlin Data Protection Commissioner successfully argued that no transborder data flow to the United States should take place even before that date unless the requirements of Articles 25 and 26 were met. Obviously, the parties to the co-branding agreement were themselves interested in finding a solution which would allow them to continue the transatlantic data processing venture after October 1998.

But it is important to stress that *we are in a pre-1998 situation.* What is legal from October 1998 and, more precisely, what is an adequate level of protection, is, to a certain extent, for the European Commission and the Article 29 Working Party to decide. This point was underlined at the European Data Protection Commissioners' Conference in April 1995 in Manchester. Although I cannot speak here on behalf of the Commission nor of the Working Party nor indeed on behalf of any other autonomous national supervisory authorities in Europe, *I am confident that the solution which was found in the RailwayCard case is very likely to pass the "adequate protection" test in 1998.*

Two separate questions

1. Does the contractual solution in the RailwayCard case meet the adequate protection requirement?
2. Can the contractual solution in this case be regarded as a model for exporting personal data from the EU to third countries in general?

The answers to these questions are not necessarily identical.

The Data Protection Agreement

In February 1996, the German Railway and Citibank signed a specific Data Protection Agreement stating that the responsibility for personal data which is collected for the purposes of the railway rests with German Railway, whereas Citibank is responsible for the protection of the credit data. Both companies have a joint responsibility with regard to the name and address of the card holder.

In order to explain the route which the data of a German RailwayCard applicant takes, and to focus on the transborder data flow aspect, I have to simplify a little. The applicants' data is captured at a train station (or travel agent) and is forwarded to Citibank Germany. After being checked it is then encrypted and sent to the Citibank subsidiary in South Dakota. This company organises the production of the card with the help of another Citibank subsidiary in Nevada. No transactional data from the use of RailwayCards with a VISA function is processed in the United States. The card is then put into an envelope with the customer's address, sealed and shipped to a Citibank subsidiary in the Netherlands from where it is mailed to the applicant's home address in Germany. (The reason for the detour via the Dutch company is simply the lower postage rates in the Netherlands compared with Germany).

The Inter-territorial Agreement

This Data Protection Agreement was followed by the Inter-territorial Data Protection Agreement (AIDP) signed by the German and American subsidiaries of Citibank.

1. The parties on both sides of the Atlantic agree to *apply German Data Protection Law* to their handling of cardholders' data.
2. Citibank in the US and in Europe is *not allowed to transfer personal data to third parties* for marketing purposes except in two cases:
   a) data of applicants for a RailwayCard with a payment function may be transferred to other Citibank companies in order to market financial services;
   b) data of applicants for a pure

RailwayCard may only be used or transferred for BahnCard marketing purposes, i.e. to try to convince the cardholder that he should upgrade his RailwayCard to have a "better BahnCard" with a credit card function.

3. The *technical requirements* on data security according to German law are spelt out in detail.
4. The American Citibank subsidiary has to *appoint data protection supervisors,* following the German legal requirements.
5. The German card customers have *all the individual rights* against the American Citibank subsidiary which they have under German law. They can ask for inspection, claim deletion, correction or blocking of their data and they can bring an action for compensation under the strict liability rules of German law either against the German Railway, the German Citibank subsidiary, or directly against the American Citibank subsidiary.
6. The Citibank subsidiaries in the United States agree to accept *on-site audits* by the German data protection supervisory authority, i.e. the Berlin Data Protection Commissioner, or his nominated agents, for example an American consulting or auditing firm acting on his behalf.

   This very important provision contains a restriction in case U.S. authorities instruct Citibank in their country not to allow foreign auditors in. However, this restriction is not very likely to happen. On the contrary, U.S. authorities have already declared, by way of a diplomatic note sent to the German side, that they will accept these audits. This decision follows an agreement between German and United States banking supervisory authorities on auditing the transborder processing of accounting data.

   This agreement very much facilitated the acceptance of German data protection audits by Citibank in the United States. As far as data security concepts are concerned, the Federal Banking Supervisory Authority and the Berlin Data Protection Commissioner will be working closely together.
7. Finally, the German Railway has been linked to this agreement between Citibank subsidiaries in a specific provision.

The conclusion I would draw to my first question on whether the contractual solution meets the "adequate protection" test would, in this particular case, be positive.

Citibank accepts high level of data protection

The company in the United States has accepted the German level of data protection. This goes well beyond all previous unilateral privacy codes and commitments drafted by American companies such as Bank America or Microsoft. In one respect Citibank even accepted a standard of protection higher than under the current German legislation! If German Railway had continued to produce the cards themselves, or to have them produced by a German company, the customers would only have had the right to object to the use or sale of their data to third parties for any *marketing* purposes. Under the Inter- territorial Agreement this is *generally* forbidden, subject to limited exceptions.

The Data Protection Commissioner insisted on the *strict purpose limitation* - that applicants' data would only be used for producing the card - since a major point in many complaints received by the Berlin Commissioner was that the data could easily be used for illegitimate purposes once it had been exported.

Furthermore, the Inter-territorial Agreement to which the data subject is not a party nevertheless gives him *individual rights which he can enforce in the German Courts.* Under German law this is a contract which directly benefits a third party.

Common law jurisdictions have legal problems with this concept. However, the Inter-territorial Agreement holds the German Citibank subsidiaries, and indeed the German Railway, responsible for any violation of the agreement and of German data protection law that might occur in the production process of RailwayCards in the United States.

What if the contract is revoked?

Of course any party to the Inter-territorial Agreement could revoke it. But this would lead

not only to claims for deletion and damages brought by the card customers but also very likely a transfer prohibition notice would be served by the Berlin Data Protection Commissioner on the German Railway.

One of the most far-reaching, important and novel provisions in the Agreement is the acceptance by the U.S. subsidiary of Citibank that on-the-spot audits by German authorities will be allowed. In practice the Berlin Commissioner is very likely, for obvious budgetary reasons, to instruct a consultancy firm in the United States with auditing experience to carry out the audit on-site. This is by no means less effective than an audit by the Commissioner himself, who has already made a visit to a Citibank data centre in Nevada.

Can contracts replace national law?

Can the contractual solution in this case be regarded as a model for legally exporting personal data from the EU to third countries in general?

Firstly, we must look at the structure of the provisions in the EU Data Protection Directive 95/46/EC concerning data export to non-EU countries.

Articles 25 and 26 of the Directive (read against the background of recitals 56 to 60) clearly state that, as a rule, the receiving *third country* has to ensure an adequate level of protection. The adequacy of the level of protection shall be assessed in the light of all the circumstances surrounding a data transfer operation; particular consideration shall be given to the rules of law, both general and sectoral, in force in the third country in question.

As a *derogation* from this rule, Article 26 provides that Member States shall allow data transfers to third countries without an adequate level of protection on the condition that either the data subject has given his unambiguous consent to the particular transfer (Article 26 para. 1a) or where the controller adduces adequate safeguards with respect to privacy protection; such safeguards may in particular result from appropriate contractual clauses (Article 26 para. 2).

Key issue: company data protection

It is quite obvious that the Directive lays down the principle that third countries, i.e. the United States, should legislate or encourage nation-wide rules and security methods to guarantee an adequate level of protection. Contractual solutions involving the data subject or private companies are only acceptable under the data export regime of the Directive in *exceptional circumstances*. Arguing in favour of standard contractual clauses as a model solution for all transborder data flows from Europe to third countries would therefore reverse the relation between the principle and the derogation under European law.

I would argue that the whole mechanism of Articles 30 and 31 of the Directive would be meaningless if the problems of adequate protection could all be solved by standard contractual clauses.

The question for the Working Party would then be: What is the standard of protection like in multinational corporations such as Citibank, Bertelsmann and Microsoft rather than what is the protection level in specific third countries? (cf. Article 30 para. 1b).

> "One of the most far-reaching, important and novel provisions in the Agreement is the acceptance by the U.S. subsidiary of Citibank that on-the-spot audits by German authorities will be allowed."

Further scepticism on contractual agreements

There are three more reasons to be sceptical towards model contractual clauses as opposed to national legislation:

1. Exceptional circumstances

The contractual solution to the German RailwayCard case was found under exceptional circumstances. The banking supervisory authorities worked as a kind of door-opener for the data protection authorities, and public protest by consumers met with a surprisingly open-minded reaction from the Citibank side. (Incidentally, during the discussions with the Commissioner, Citibank turned out to be much more flexible and privacy-minded than their partners from the state-owned German Railway).

It is uncertain whether future proposals to export personal data from the EU to a third country will be made by corporations who in each case attach similar importance to data protection principles as Citibank did here.

2. A level playing field

Moreover, personal data will not only be exported by large multinational corporations with their well-staffed legal departments which can draft sophisticated webs of contractual obligations. Small and medium-size enterprises will also play a role in the global market-place. Small and medium-size enterprises very often do not have the legal knowledge at their disposal to meet the requirements of Articles 26 (2) as interpreted by the Commission and the Member States. Only the national legislature can provide for equal conditions of competition.

3. Maintaining uniformity of standards

The creation of a national mechanism to oversee the private sector is essential in large data-importing third countries such as the United States and Canada. The contractual solution just described cannot provide for such a mechanism. On the contrary, it may lead to many different supervisory authorities from foreign countries initiating audits in the third country, thereby applying different instead of uniform standards.

Conclusion: contracts cannot replace national law

Multinational corporations such as Citibank can and will play an important standard-setting role in the global market-place. It will take considerable time until an adequate level of protection in terms of general and sectoral rules of law has been ensured in all third countries importing personal data from Europe.

In this transitional period, standard contractual clauses may, in exceptional circumstances, prove to be useful. In any case they should at least contain the same safeguards as the German RailwayCard Agreement. However, contractual standard-setting by private corporations can only complement and support but never replace national legislation.

This is an edited version of a presentation by Dr. iur. Alexander Dix, LL.M. (Lond.) Data Protection Deputy Commissioner Berlin, Germany who addressed the 18th International Data Protection Authorities Conference in Ottawa in September 1996. Contact details: Berliner Datenschutzbeauftragte, Pallasstrasse 25, Berlin, 10781 Germany

Tel: +(49) 30 7876 8828
Fax: +(49) 30 216 9927