GERMAN DPA'S REVISE GUIDELINES FOR MANAGING TRANSBORDER DATA FLOWS

On October 27/28th, the Dusseldorf Circle, the regular meeting of German Lander (state) Data Protection Authorities, revised their checklist of recommended steps to be taken by private sector organisations transferring personal data abroad. The original and revised documents were drafted by its transborder data flows (TBDF) committee, chaired by Dr. Dieter Baumeister, the head of the data protection supervisory authority for Berlin. Their review of the document, published a year earlier, followed mainly negative comments from companies and industry associations. The revised document has not been published but a change was that of description from "checklist" to "guideline." This change indicates that the DPA's now see the document as an interim measure outlining their recommended interpretation of the German Data Protection Act's requirements for transborder data flows, until the EU data protection directive enters into force in national law. The TBDF committee of the Dusseldorf Circle will then revise the document again.

The current legal basis for TBDF

Personal data is transferred in large quantities by private sector organisations from Germany to other countries. Under German law, these transfers are considered as communication to a third party.

The EU Data Protection Draft Directive has not yet been adopted and it will take some time before it is implemented in national law. The question of how to ensure the protection of data subjects' legitimate interests and rights once their personal data crosses national borders, remains open.

The current legal basis for data transfer abroad is the Federal Data Protection Act, § 28 ss. 1 and 2, as well as, § 29 ss. 2, unless sector specific regulations take precedence.

Weighing of different interests needed

The fact that data transfers take place to countries which do not offer a sufficient level of data protection has to be taken into account when weighing the legitimate interests of data subjects, in the context of the above quoted sections of the Act. An agreement between the exporter of personal data based in Germany and the recipient abroad, with the aim of protecting the data subject's rights, does not have absolute value. It is *only one* of the relevant factors when considering legal requirements for transfers of data abroad.

Such an agreement may be particularly relevant in cases of data transfers:

- without the consent of data subject, and
- which are also not necessary for the fulfilment of a contract with the data subject.

Guideline should reduce data risks

The guideline may be useful in assessing the legality of such transfers. Its aim is to improve the protection of data subjects, which is essential where there are data protection deficiencies in the data recipient's country. It provides the private sector organisations with an instrument for evaluating data transfers.

The guideline should be handled flexibly and according to individual circumstances. The intention was not to set up a fixed model contract, but to adopt additional data protection measures to reduce the risks to the data subject caused by transborder data flows.

The Guideline

1. Co-operation between the data exporter and data importer

The data exporter shall investigate the legal situation with regard to data protection in the recipient country. The first step would be to contact the competent authorities in the recipient country and the data recipient. Then the exporter must assess whether the country has a sufficient level of data protection, by taking into account all elements of the individual case:

- category of data
- purpose, context and usage
- duration of the intended processing
- general or sectoral legal regulations in the recipient country
- codes of conduct in the recipient country.

If the data exporter does not undertake inquiries in spite of the unclear situation in the recipient country, or if the situation concerning data protection still remains unclear in spite of such inquiries, it has to be assumed, if in doubt, that the recipient country does *not* provide an adequate level of data protection.

2. Purpose and use of the data

The purpose for which the data is to be used should be fixed by the contract in a clear and binding manner. The data exporter and the recipient should agree on prohibiting the use of data for any other purpose. In appropriate circumstances, as a means of clarification, certain inadmissible uses may be cited as examples of prohibited uses.

3. Rights to information

In the interests of the best possible transparency, the data subject should have a right of information with the recipient abroad as well as with the German data exporter. This aim, however, can only be accomplished effectively if the data recipient is bound by contract to provide the relevant information to the sending party. Otherwise, the latter would hardly be in a position to provide the data subject with the information required.

4. Rectification, blocking, erasure

The data subject should have the choice of invoking these rights either against the recipient abroad or against the data exporter based in Germany. Where these rights are used against the sending party, its co-operation is required in fulfilling the duties of the recipient party. This presupposes that the sending party has obtained a right to rectification, blocking and erasure from the recipient party.

5. Notification duty

It is specially important that, beyond the requirements of § 33 BDSG, the sending party is obliged to notify the data subject of the data transfer abroad. In particular, the data subject has also to be informed about the rights he has obtained by the contractual agreement between the sending and the recipient party.

6. Data security

Data security measures should be made a contractual obligation for the recipient. The level of security is primarily dependent on the sensitivity of the data. The data security provision of the German Act (Art. 9), including the Act's appendix, may serve as a starting point for guidance in this respect.

7. Checking the agreement's implementation

The data exporting party must be in a position to check, among other things, the implementation of the contractual agreements mentioned above, in particular:

- the rights of the sending party to obtain or to have access to information and, if necessary,
- rights to on-site inspections by the exporter.

The appointment of a data protection controller might also be worth considering.

8. Penal clause

The data recipient should be bound to pay a penalty to the data sender in the event that the recipient party does not meet its contractual obligations. This too, should strengthen the willingness of the recipient party to observe the rights of the data subject.

9. Liability

The interests of the data subject would receive increased attention if the exporter and the data recipient were under joint and several liability. One might consider a joint and several bond between the exporting and the recipient party, with the data subject being informed about the contents of the contract. Without this, the data subject would not be able to use the rights he obtained, due to his ignorance of them. In cases of transfer of especially sensitive data, a clause on strict liability may also be included.

Privacy Laws & Business is grateful to Dr Herbert Burkert of GMD, Germany, for translating and interpreting this document.