MAYER·BROWN

New EU Standard Contractual Clauses
for Commissioned Data Processing

New EU Standard Contractual Clauses

September 2010

European companies wishing to transfer data outside of the EU have different ways to guarantee a data protection level similar to that of Europe in the third country. The EU Commission's standard contractual clauses have proven to be of value in practice as they are not subject to the authorization requirement by the competent supervisory authorities.

In the meantime, the EU Commission has passed new standard contractual clauses for commissioned data processing, the use of which is compulsory for new commissioned data agreements as of May 15, 2010. Prior agreements must be adjusted if the manner of the commissioned data processing changes. For the first time the new standard contractual clauses permit a subcontracting; this is, however, subject to stringent requirements.

This white paper provides an overview of the new standard contractual clauses and the implementation thereof in Germany, the United Kingdom and France.

Tim Wybitul
Partner, Frankfurt
T: +49 69 79 41 2231
twybitul@mayerbrown.com

Dr. Andrea Patzak
Associate, Frankfurt
T: +49 69 79 41 1067
apatzak@mayerbrown.com

German Law Perspective

Recently, the European Commission passed new standard contractual clauses for the transfer of personal data to commissioned data processors located in countries outside of the European Union (EU) and the European Economic Area (EEA), so called third countries. As of May 15, 2010, the former contractual clauses provided by the EU Commission may no longer be used. The EU standard contractual clauses are probably the most-used instrument in order to legitimize the transfer of personal data to third countries. This overview shows which requirements are set out for cross-border data transfers and how companies can fulfill these requirements.

MEANING OF COMMISSIONED DATA PROCESSING FOR EUROPEAN COMPANIES

It is often an economic necessity for, for example, German companies to transfer personal data to recipients in third countries. Reasons for this need include out-sourcing projects, centralized data-bases and joint ventures. Frequently, European companies conclude IT-Outsourcing agreements with service providers in third countries. In the realm of such IT services the instructed service provider often gets access to personal data (e.g. the instructor's company's employees). From a legal point of view such facts present a transfer of personal data into a third country. According to Sections 4b and 4c of the Federal Data Protection Act (*Bundesdatenschutzgesetz, BDSG*), such cross-border transfers are only permitted under strict provisions.

THE TERM "TRANSFER"

Transferring is providing data to a third party. A third party is any person or agency which is not part of the transferring company. In business, third parties are, for example, employees of other companies or other persons from outside of the principal company. The German data protection law stipulates the same requirements for the transfer of data within the same group of companies as for every other transfer; it does not recognize a privilege for the group of companies.

A transfer can also be both, the passing on personal data to a third party and the keeping data available for a third party to view or to request on demand. The data is transferred to the third party as soon as the third party views or demands the data.

STRINGENT REQUIREMENTS FOR THE PERMISSIBILITY OF TRANSFERS

German data protection authorities examine the permissibility of a data transfer into third countries via a two-level evaluation.

First Level Permissibility Examination

In the first level evaluation, the data protection authorities will determine whether the planned transfer of personal data to a third party would be permissible according to the BDSG's common standards. Generally, the BDSG prohibits handling personal data, unless a statutory regulation or a valid consent by the affected person permits this handling of data.

A typical example of transferring personal data in accordance with the BDSG's common standards is if the transfer is required to maintain the legitimate interest of a company according to Section 28 Subsection 1 Clause 1 No. 2 BDSG. Additionally, there may not be any reason to assume that the affected person whose data is being transferred has a legitimate interest in excluding the transfer which outweighs the company's interest.

The company must have a legitimate economic interest for the transfer. For example, lowering costs can certainly be such a necessary business reason.

Furthermore, a transfer according to Section 28 Subsection 1 Clause 1 No. 2 BDSG can only be effected if it is "necessary" to maintain the economic interest. That means that the transferring company can only transfer the data which is truly necessary to realize the legitimate business purpose.

The most important part of this legal examination is to determine whether the interests of the persons affected by the transfer are adequately protected. At this time the authorities weigh the company's interests against those of the person whose data is to be transferred.

In practice, for example, it is advisable that companies look for precedents for permissible transfers (such as from adjudication, or activity reports by the state's supervisory authorities) and to use these standards as a guide.

If all of these requirements are fulfilled, then the transfer to another company in Germany, the EU or the EEA are permissible. The transfer to another company in a third country is, however, only permissible under stringent requirements. These are detailed below.

Second Level Permissibility Examination

Even if a transfer of personal data is permissible within Europe according to the BDSG's common standards, this does not mean that the transfer automatically would be permissible to a third country without an adequate level of protection. Here, Section 4c BDSG states far more stringent requirements than those that apply to intra-German or intra-European transfers. Therefore, an adequate data protection level through additional means must be created in order to permit the transfer, or there must be an exception regulation, which permits the data transfer even without a previous creation of an adequate data protection level.

Companies often use the standard contractual clauses passed by the EU Commission in order to fulfill these requirements. In contrast to those binding company provisions named in Section 4c Subsection 2 Clause 1 BDSG (Binding Corporate Rules – BCRs) the EU standard contractual clauses do not need to be authorized from the responsible supervisory authority in order to facilitate a permissible data transfer into third countries.

These binding standard contractual clauses seek to establish a uniform standard in order to facilitate cross-border data transfers into third countries in a timely manner without bureaucratic delay. In the past, data protection supervisory agencies held different positions on whether standard contractual clauses needed to be presented to the supervisory authority individually or even needed to be examined and authorized at all.

The so called *Düsseldorfer Kreis* determined that by using the standard contractual clauses completely and unchanged there is neither an obligation for authorization from nor an obligation for disclosure to the supervisory authorities. The *Düsseldorfer Kreis* is the joint panel for the data protection supervisory authorities of the individual federal states. In Germany, the representatives of the supervisory authorities for the private sector are organized at state level and together form the *Düsseldorfer Kreis*. Therefore, usually the decisions rendered by the *Düsseldorfer Kreis* are decisive for the supervisory authorities.

THE DIFFERENT TYPES OF STANDARD CONTRACTUAL CLAUSES

Prior to the new standard contractual clauses decision, the EU Commission had decided on three sets of standard contractual clauses. The first two, dated June 15, 2001 and December 27, 2004, refer to "normal" transfers to another competent authority in a third country. The third set of standard contractual clauses for the transfer of personal data to commissioned data processors, dated December 27, 2001, deal with data transfer to data processing service providers who process data in commission for the data controller. Section 11 BDSG covers making personal data available to commissioned data processors in an intra-German or intra-European connection. Such a commissioned data processing in third countries is, however, not envisioned by Section 11 BDSG.

The previous standard contractual clauses for commissioned data processing in third countries are no longer applicable for agreements concluded as of May 15, 2010. However, agreements with the old standard contractual clauses which are already concluded remain valid and do not need to be automatically amended to fit the EU Commission's decisions. If, however, the contracting parties wish to agree upon changes to existing agreements regarding commissioned data processing in third countries, or if the principal wishes to award a subcontract, then the parties must conclude a new agreement using the new standard contractual clauses.

NEW REQUIREMENTS FOR CROSS-BORDER COMMISSIONED DATA PROCESSING

Requirements for Subcontractor Relations

Currently, under certain circumstances, the agent can enter into subcontractor relations on the basis of the new standard contractual clauses. That was not ruled in the previous standard contractual clauses for the transfer to commissioned data processors in third countries. The lack of such a regulation in the old standard contractual clauses was severely criticized.

Such subcontracting is, however, subject to certain permissibility requirements:

- Before entering into a subcontract the principal must agree to it in writing.
- This agreement must obligate the subcontractor in the same manner that the agent in the main agreement is obligated.
- The agent must remain fully liable to the principal for all contractual violations by the subcontractor. Agent and subcontractor must agree upon a so called third party beneficiary clause (*Drittbegünstigtenklausel*), under which affected persons must also be able to assert claims for damages against the subcontractor, if necessary.
- The law of the country in which the principal is based must also be the applicable law, just as in the old standard contractual clauses. The data protection laws applicable to the principal must now also apply to data processing by the subcontractor. If a German company transfers data to an agent in a third country who, in turn, passes on some of the data to a subcontractor, then German law also applies to the agreement between the agent and the subcontractor.
- Additionally, the contractual relations with the subcontractors must be carefully documented. The agent must both inform the principal and obtain written authorization prior to a subcontracting and must also provide the principal with additional copies of the subcontracts.
- Finally, the principal must annually maintain a current index of the agreements with subcontractors and make this index available to the relevant supervisory authorities. It is not clear whether this can be merely a list of the existing sub-contracts, or whether the index must also contain the respective clauses. However, it can be assumed that the agent does not need to disclose the agreements with the subcontractors. According to the opinion of the *Düsseldorfer Kreis* the principals do not need to disclose to the supervisory authorities the standard contractual clauses between principal and agent. Therefore, this suggests that a subprincipal does not need to disclose the standard contractual clauses executed with the subagent, which must contain the same provisions as those of the concluded standard contract clauses of the relationship.

Applicable Law for the Data Processing Contract

The standard contractual clauses only refer to data protection law provisions. A complete agreement regarding commissioned data processing in a third country must also cover substantial economic aspects, which the principal and agent can determine in the remaining agreement[1]. The wording of the standard contractual agreement and the recitals by the EU Commission prescribe that the standard contractual clause (which refers to data protection in transfers) is subject to the law of the country in which the principal is based. Now, data processing contractors are also subject to the principal's applicable data protection laws. However, the other (economic) provisions can be subject to another legal system by making the standard contractual clauses a separate appendix to an outsourcing or service agreement. This appendix can then – regardless of the main agreement – be subject to the law of the country in which the principal is based. It remains to be seen what position the supervisory authorities will take regarding this procedure.

IMPLEMENTATION OF THE NEW STANDARD CONTRACTUAL CLAUSES IN CONTRACTUAL CHANGES

The supervisory authorities will probably apply a more stringent measure regarding whether the old standard contractual clauses may be further used or the new standard contractual clauses must be implemented because there was a minor change to the existing agreement. It can be expected that every amendment of the agreement will be assessed as a contractual amendment within the meaning of the EU Commission's decision.

Whether such a minor change applies to agreements that consist of numerous contracts is not easy to answer, especially regarding comprehensive IT service agreements, which, for example, deal with data processing in an EU/EEA foreign country. Such agreements usually consist of a master services agreement and numerous appendices, which define the subject matter of the agreement more closely regarding definitions, statements of work, service level agreements, pricing terms and other comparable provisions.

EFFECTS ON COMPANIES

Companies should respond to this changed legal situation by thoroughly examining whether and how they should use the new standard contractual clauses. Existing contractual clauses should be examined to determine if changes to contract terms, appendices or amendments can require the use of the new clauses. Most importantly, the scope of the contractual changes should be considered. Failure to take these steps can lead to penalties, claims for compensation damages and, above all, substantial injury to public image if it appears the company is not serious about data protection.

[1] EU Commission, Decision 2010/87/EU, recital 4, ABl. EG Nr. L 39 dated February 12, 2010, 5(5).

Mark A. Prinsley
Partner, London
T: +44 20 3130 3900
mprinsley@mayerbrown.com

Oliver Yaros
Associate, London
T: +44 20 3130 3698
oyaros@mayerbrown.com

UK Law Perspective

The UK takes a similar approach to that in Germany and other EU member states in that the UK's Data Protection Act prohibits the transfer of personal data by entities in the UK to a recipient in a country determined by the European Commission as not offering an adequate data protection regime outside of the EEA except in where a limited number of circumstances apply.

The UK regulator for data protection, the Information Commissioner's Office (ICO), has authorized two sets of the EU standard contractual clauses as providing a legitimate way to export personal data out of the EEA. The first set is to be used when a UK entity, being a data controller (a person that determines the purposes for which and the manner in which any personal data are, or are to be, processed) exports personal data outside of the EEA to a data processor (a person who processes the data on behalf of the data controller) and the second set is to be used to govern transfers from one data controller to another outside of the EEA.

As in Germany and elsewhere in the EU, the first set have now been replaced as of May 15, 2010 by a new set of EU standard contractual clauses which must now be adopted where any new arrangement is going to be entered into, and as explained above, the new first set of standard contractual clauses allows for the data controller to authorize the data processor to subcontract its processing obligations to a third party on the conditions set out in the new first set of model terms.

However, unlike in Germany, there is no two tie-examination for data controllers in the UK before exporting data based on the EU standard contractual clauses. The German Data Protection Act provides for more specific requirements regarding the compliant transfer of personal data to any third country. Data controllers must satisfy themselves that their use of the personal data will meet the general standards set out in the Data Protection Act that governs how personal data may be fairly and lawfully processed by them. The ICO retains the right to investigate the arrangements a data controller has made should it receive a complaint and/or wish to investigate.

Data controllers that had entered into export arrangements with data processors on the previous first set of model terms before May 15, 2010 may continue to export personal data under those arrangements unless the types of data processing operations or data transfers are going to be changed or where the data controller intends to authorize its data processor to subcontract its processing obligations to a third party.

Laurence Dumure Lambert
Partner, Paris
T: +33 1 53 53 43 43
ldumurelambert@mayerbrown.com

Régine Goury
Of-Counsel, Paris
T: +33 1 53 53 43 43
rgoury@mayerbrown.com

French Law Perspective

As in the other European Union Member States, the French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés, CNIL*) controls transfers of personal data from a data controller to a data processor located in a recipient country outside the European Union, where the law of such recipient country fails to provide an adequate level of protection of the data transferred, as determined by the European Commission.

The CNIL must authorize transfers of personal data to recipient countries which have not been recognized by the European Commission as granting an adequate level of protection of personal data. For this purpose, the CNIL reviews the contractual clauses or the binding rules which the companies have entered into to govern the transfers of personal data outside the European Union.

The French Data Protection Law provides a view exceptions, for example if the individual has expressly agreed to such transfer or if the transfer is necessary to the safeguard of this individual's life or the safeguard of the public interest. But these exceptions are strictly interpreted by the CNIL since they trigger a lack of protection of the personal data in the recipient country. The CNIL recommends that such exceptions be limited to exceptional cases where it would be inappropriate, even impossible, to implement a transfer of personal data based upon contractual clauses (or internal rules).

The transfer of personal data to countries outside the European Union must meet a number of requirements defined by law:

- the data processing itself must have been previously filed with the CNIL;
- the transfer must have a determined, express and legitimate purpose;
- the personal data transferred must not be subsequently used in a way contrary to the purpose of the data processing;
- the personal data transferred must be adequate, relevant and not excessive considering the purpose of the transfer.

For example, the CNIL highlighted that worldwide companies frequently contemplate transfers of data relating to the whole of the company's staff to centralize human resources databases at the group level. Such transfers sometimes relate to the whole of the employees' personal data, including data which appear to justify a mere local treatment. Such transfers may trigger issues with respect to the legitimacy and relevance of the personal data in light of the purpose of the transfer.

In any case, the individuals whose personal data are likely to be transferred must be informed of the existence of the transfer in details, including the purpose of the transfer, the recipient country, the categories of recipients of the data and, as the case may be, the type of protection granted (contractual clauses, internal rules, Safe Harbor certification, etc.).

Pursuant to French labour law provisions, the data controller's Works Council must also be informed of the data processing relating to the human resources together with any amendment or transfer thereof outside the European Union.

Where a data controller transfers personal data to a data processor to a country, located outside the European Union, the law of which does not provide for any adequate protection of personal data, it is recommended to use the standard contractual clauses set by the European Commission to facilitate the filing process with the CNIL, although no provision forbids the recourse to any other clauses. The CNIL promotes the recourse to such standard contractual clauses for more legal security and also to fasten the authorization process.

The CNIL has favorably considered the adoption by the European Commission of a new set of standard contractual terms as of May 15, 2010 for the transfer of personal data by a data controller to a data processor located outside the European Union, enabling subsequent transfers of personal data to sub-processors located outside the European Union under certain conditions. Such new standard contractual clauses will indeed facilitate in practice chains of transfers of personal data and thus avoid unnecessary filings of contractual clauses with the CNIL for each sub-transfer as has been the case hitherto.

It should be noted that this new decision of the European Commission only relates to the transfer of personal data by a data controller to a data processor located outside the European Union and does not consider the situation where the data processor is located in the European Union but subcontracts to a data processor located outside the European Union. We understand that discussions are underway within the G29 in this respect.

About Mayer Brown

Mayer Brown is a leading global law firm with offices in major cities across the Americas, Asia and Europe. We have approximately 875 lawyers in the Americas, 300 in Asia and 425 in Europe. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest investment banks. We provide legal services in areas such as Supreme Court and appellate; litigation; corporate and securities; finance; real estate; tax; intellectual property; government and global trade; restructuring, bankruptcy and insolvency; and environmental.

OFFICE LOCATIONS

AMERICAS
- Charlotte
- Chicago
- Houston
- Los Angeles
- New York
- Palo Alto
- São Paulo
- Washington

ASIA
- Bangkok
- Beijing
- Guangzhou
- Hanoi
- Ho Chi Minh City
- Hong Kong
- Shanghai

EUROPE
- Berlin
- Brussels
- Cologne
- Frankfurt
- London
- Paris

ALLIANCE LAW FIRMS
- Spain, Ramón & Cajal
- Italy and Eastern Europe, Tonucci & Partners

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.