October 13, 2015

Practice Group(s):

Labor, Employment and Workplace Safety

Cyber Law and Cybersecurity

Transfer of Employees' Personal Data from Germany to the United States under German Data Privacy Law

By Nicolas Roggel and Dr. Friederike Gräfin von Brühl

The Issue

Following the ECJ's decision in the *"Schrems"* case which has invalidated the Safe Harbor framework (click here for our firm's recent alert on this matter) multinational corporations may now face profound privacy law related compliance issues in a multitude of jurisdictions.

In the Schrems decision, the ECJ held that the widespread practice of U.S. companies to self-certify under the Safe Harbor standards in order to legitimize data transfers from EU companies to U.S. companies does not provide for an adequate level of data protection. As a result the court held that the Safe Harbor principles are invalid and thus shattered the legal basis for the data transfer from countless EU entities to U.S. entities. The ECJ substantiates its decision with the fact that all personal data stored in the United States is subject to almost unrestricted and unpredictable access by U.S. authorities, that the data subject has no legal way to prevent this access, and that subordination under the Safe Harbor statute does not mitigate this threat. The ECJ considers this situation to be a major and unjustifiable violation of EU citizens' fundamental rights and requires local data protection authorities to assess the admissibility of data transfers without relying on the subordination of U.S. companies under the Safe Harbor regime.

In Germany, the transfer of employees' personal data to U.S. group companies had already been a highly problematic and recurring issue in the past. After the ECJ's decision, the magnitude of this issue has significantly increased.

Transfer of personal data from Germany to the United States must comply with these regulations:

- general provisions for handling personal data under German data privacy law, and
- legal provisions for a cross-border transfer to a country outside the EU/EEA.

Both requirements can constitute high legal hurdles and may often disrupt or complicate the common approach of seamlessly integrated and efficiently operating multinational corporations.

General Legal Requirements for Handling Employees' Personal Data

As a first step, the transfer of employees' personal data must comply with the general provisions for the handling of personal data under German data privacy law. German data privacy law is among the strictest in the world requiring specific justification for any handling of personal data.

Transfer of Employees' Personal Data from Germany to the United States under German Data Privacy Law

In the context of employment relationships, the BDSG *(German Federal Data Protection Act)* provides for a number of specific statutory justifications. A key element of such justifications is the balance of the collector's (i.e., the company's) and the data subject's (i.e., the employee's) interests whereby individual privacy rights are considered fundamental constitutional rights.

General Legal Requirements for a Cross-border Transfer of Personal Data from Germany to the United States

In addition to the general legal justification for handling personal data, a data transfer to a country outside the EU/EEA is allowed only if an adequate level of data protection is guaranteed. The level of data protection in the United States in general is not considered adequate by the German data protection authorities. Therefore, U.S. entities must ensure an adequate level of data protection themselves.

Safe Harbor framework

Previously, U.S. entities could guarantee the necessary level of data protection by joining the Safe Harbor agreement. Following the ECJ's *Schrems* decision, this is no longer possible.

Standard contractual clauses and binding corporate rules

Without the option of Safe Harbor, the legal admissibility of the data transfer to the United States depends on obtaining authorization by the competent supervisory authority in Germany. In order to obtain this authorization, sufficient safeguards with respect to the protection of privacy must be presented to the authority. These conditions can possibly be met by using the standard contractual clauses set out by the European Commission or by establishing binding corporate rules governing the processing of personal data within the affected group entities. When using the standard contractual clauses set out by the European Commission without modification, a separate authorization by the German competent supervisory authority was—at least until now—not required. In the light of the ECJ's decision, however, it is highly doubtful that this authorizing effect of the standard contractual clauses can be upheld. A number of competent German authorities have already expressed the view that, following the ECJ's reasoning in the *Schrems* decision, the standard contractual clauses or binding corporate rules may no longer be sufficient to ensure an adequate level of data protection at the affected U.S. entity. They take the position that the same reasons that have been found to render the Safe Harbor solution to be noncompliant may be likely to also override any EU standard clauses and binding corporate rules.

Therefore, relying on standard contractual clauses or binding corporate rules will most likely not be a sustainable and thus practical approach in Germany.

Individual Consent

Individual consent can offer a solution for both the handling of personal data in Germany and its cross-border transfer to the United States. However, such consent must be obtained from all individuals concerned. In employment situations therefore consent will be required from all affected employees.

Such consent requires careful drafting as German data protection law requires "informed consent" based on comprehensive explanations being provided regarding the handling and transferring of personal data. Specifically, detailed explanations regarding the cross-border transfer and the treatment of the personal data in the United States will be necessary. For a valid consent, employees must be expressly informed that their data may be subject to unnoted regulatory access, e.g., by the U.S. National Security Agency.

Further, the employee concerned must grant consent in writing and voluntarily. The consent should not be included in the employment agreement. Rather, a separate document should be signed afterwards. In the past, it has been questioned whether an employee can ever be in the position of granting voluntary consent in the context of an employment relationship due to their lack of independence. However, a recent decision by the German Federal Employment Court may be understood in a way that, in principle, an employee might be able to grant voluntary consent in the context of their employment relationship. However, the validity of such consent and in particular the employee's (in)dependence has to be assessed in every single case.

Obtaining a collective consent for all employees from the works council is not possible. Further, it is highly doubtful that a cross-border transfer to the United States can be justified by agreeing a works agreement with the works council without need for authorization by the competent supervisory authority in Germany. Authorization for such works agreement is most likely not to be expected for a transfer to the United States.

If valid individual consents from all employees can be obtained, it will not be necessary to rely on the statutory justifications in the BDSG, the Safe Harbor framework, standard contractual clauses or binding corporate policies.

Summary

When it comes to the transfer of employees' personal data from Germany to the United States, only employees' valid consent declarations may currently ensure a reasonable degree of legal certainty.

The need to rely on employees' willingness to grant individual consent is likely to be unacceptable or impractical for many multinational corporations. Therefore, immediate action by the appropriate EU, U.S. and national authorities and legislators is necessary in order to ensure continued economic activity and growth in the transatlantic economic area.

Authors:

Nicolas Roggel
nicolas.roggel@klgates.com
+49.30.22.00.29.305

Dr. Friederike Gräfin von Brühl
friederike.bruehl@klgates.com
+49.30.22.00.29.415

Transfer of Employees' Personal Data from Germany to the United States under German Data Privacy Law

K&L GATES

Anchorage Austin Beijing Berlin Boston Brisbane Brussels Charleston Charlotte Chicago Dallas Doha Dubai Fort Worth Frankfurt Harrisburg Hong Kong Houston London Los Angeles Melbourne Miami Milan Moscow Newark New York Orange County Palo Alto Paris Perth Pittsburgh Portland Raleigh Research Triangle Park San Francisco São Paulo Seattle Seoul Shanghai Singapore Spokane Sydney Taipei Tokyo Warsaw Washington, D.C. Wilmington

K&L Gates comprises approximately 2,000 lawyers globally who practice in fully integrated offices located on five continents. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit www.klgates.com.