IADC COMMITTEE NEWSLETTER

EMPLOYMENT LAW

March 2017

IN THIS ISSUE

The article illustrates the aspects to keep in mind when transferring personnel data within a company group structure. First, the requirements for a data transfer in Germany are explained differentiating between data transfers that do not need justification and those that do. Based on these principles, the additional requirements for transmission to a foreign country are demonstrated distinguishing between EU/EEA and non-member countries. Additionally, the special case for the USA is mentioned to provide an outlook on the future of the EU general data protection regulation.

Personnel Data within the Group – An Internal Matter (or Not)? A European/German Perspective

ABOUT THE AUTHOR

Gerlind Wisskirchen is a partner and certified employment and labor lawyer in employment at CMS Hasche Sigle in Cologne, Germany. She advises German and foreign multinational companies on all areas of individual and collective employment law. She has particular expertise in cross-border aspects and heads corresponding European projects such as cross-border transfer, reorganizations of businesses (outsourcing, off-shoring), issues of compliance, cross-border audits and compliance and internal investigations with regard to compliance issues, company co-determination, matrix structures of multinational companies, European works councils, the implementation of codes of conduct and whistleblowing systems, the assignment/relocation of employees, data privacy issues and holistic production systems (Toyota business system). She can be reached at gerlind.wisskirchen@cms-hs.com.

ABOUT THE COMMITTEE

The Employment Law Committee serves members who represent employers and their insurers. Committee members publish newsletters and Journal articles and present educational seminars for the IADC membership-at-large and mini-seminars for the committee's membership at the Annual and Midyear Meetings. The Committee presents significant opportunities for networking and business referrals. The goal of the Employment Law Committee is to build an active committee with projects that will attract and energize attorneys who practice employment law on a domestic and international basis. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Marion Walker
Vice Chair of Publications
Law Office of Marion F. Walker
marionfwalker@gmail.com

Introduction

The group headquarters' e-mail seemed unspectacular at first glance: "Please provide us with a complete list of all employees working at your company including details regarding age, entry date, position and remuneration by tomorrow, COB." The HR department addressed was able to quickly compile the list and send it to headquarters, without further inquiry. It was overlooked – as is often the case – that this transfer entails significant risks under European data protection law. Data transfers between group companies are often regarded as "internal matter." This holds true, in particular, when the parent company cites reasons for the inquiry that seem plausible: be it conducting a due diligence review, introducing group-wide know-how databases or group-wide staff development.

The transfer of personal (employee) data between legally independent companies of a group is not necessarily permissible under data protection law. The European Data Protection Law permits the collection, processing and use of personal data only if this is permitted by law or if the data subjects have given their consent. Corporate and economic connections and links between the sender and the receiver of personal data are not taken into consideration; companies belonging to the same group, especially, are not considered one entity. If the transfer of personnel data does not satisfy the requirements under data protection law, it may, e.g. in Germany, result in fines of up to EUR300,000.

This cannot be dismissed as a purely theoretical problem (any more). The supervisory authorities have intensified their activities and increasingly imposed fines – on companies and on the acting employees and the responsible managing directors and board members as well.

The problem is aggravated by the EU General Data Protection Regulation, which will be applicable as of 25 May 2018. According to the General Data Protection Regulation, even fines of up to EUR20 million or 4 percent of the annual turnover – possibly of the entire group – may be imposed.

I. Current Situation Using the Example of Germany

Data protection law does not facilitate the exchange of data within group structures; there is thus no "group privilege". Transfers between legally independent companies, belonging to the same group, are treated the same as transfers to third parties by the law. Under German data protection law, each company is deemed an independently responsible party (§ 3 (7) of the Federal Data Protection Act).

A. Data Transfer in Germany

Transfer of personnel data is tantamount to data processing and requires justification.

1. Contract Data Processing Is Not a Transfer of Data

Data transfer covers both passing on and providing data for inspection or retrieval (§ 3 (4) No. 3 of the Federal Data Protection Act). Whether personnel data are forwarded by e-mail or whether other companies are granted direct access to the specific server is therefore irrelevant.

Contract data processing, however, lacks a transmission process (§ 11 of the Federal Data Protection Act). A contractually tied contract data processor is not considered a "third party." Examples of contract data processing include externally provided salary statements, saving data in the cloud or providing similar IT services. The instruction to process data must be given in writing, heeding the statutory minimum content pursuant to § 11 of the Federal Data Protection Act. An essential criterion regarding contract data processing **is the contractor's duty to comply with instructions. A contract data processor may not have discretionary power** with regard to the manner in which the data are processed – as is the general case for salary statements, for example. **The parent company may also function as contractor.** It then, however, has to fulfil a purely "serving function" and submit to the instructions of the companies belonging to the group.

If the data processor has decision-making powers or if the principal's exertion of influence is limited, the contract data processor is considered the controller within the meaning of the Federal Data Protection Act. This is then deemed to be a transfer that requires separate justification.

It may be difficult to make a distinction in individual cases. Since supervisory authorities are rather critical of activities exceeding the mere provision of salary statements, it is paramount to review the individual case thoroughly.

2. Justification of Transfer

If a case in which data are transferred is not a case of contract data processing, justification is required. A transfer of personnel data may be permitted based on a statutory regulation or the employees' valid written consent.

a) Consent

At first glance, the employees' consent may be the preferred choice, especially since standardized employment agreements often include such clauses.

However, such forms of consent rarely satisfy the strict requirements set out in § 4 a of the Federal Data Protection Act. The supervisory authorities and some legal scholars fundamentally doubt that consent given in the employment agreement, as required under § 4 a of the Federal Data Protection Act, actually can be based on "the free decision of the data subject." This doubt was, however, countered by a recent decision (11 December 2014 – 8 AZR 1010/13) of the Federal Labor Court (BAG)

that emphasized that employees do not lose their fundamental and personal rights when they enter into an employment relationship and are integrated into an establishment.

Besides, standardized clauses in employment agreements often do not satisfy the requirements for valid consent: for one, "informed consent" would have to include a sufficiently clear reference to the specific purpose of the data processing and in general to the consequences of refusing to grant consent. For another, the employee would need to have a real choice between granting and refusing consent. It is therefore (and owing to the necessary revocability of any consent with effect for the future) difficult to establish standardized processes in HR based on consent.

b) Statutory Regulations

Statutory regulations that may permit transfer are primarily to be found in the Federal Data Protection Act.´

aa) Necessary for the Employment Relationship

For the duration of the employment relationship, § 32 of the Federal Data Protection Act applies primarily. Accordingly, transfer is permissible if this is necessary for the decision on hiring, performing the employment contract or terminating the employment relationship.

It primarily relates to the legal relationship to the employer, meaning the contracting company. The purposes pursued by a company affiliated with the employer are generally irrelevant. Transferring employee data can thus only rarely be based on § 32 of the Federal Data Protection Act.

Exceptions are accepted, if the employment relationship is already closely connected to the group at the time the agreement is concluded. A prime example is agreeing on a group-wide mobility clause: such a clause entitles the employer, for example, to transfer personnel data for the purpose of group-wide human resources management. This also applies to executive employees who were aware of the group structure and their positions' group connection. The Clause justifies the transfer of their personnel data for standard group incentive programs, or performance evaluation and personnel development systems. Such group connection may be created even after the employment relationship has been established.

The general permissibility does not mean, however, that all personnel data can be transmitted freely. It has to be determined in the specific individual case whether the transfer is "necessary" for the purpose of the employment relationship. A group connection alone will therefore not suffice to justify the transfer of personnel data for a due diligence review, when preparing a sale of companies or establishments. In this and similar cases it should be considered whether an anonymous data transfer would not be sufficient to fulfil the intended purposes. The advantage is that the

personal reference no longer exists, so that the strict provisions under data protection law are no longer relevant.

bb) Employer's Prevailing Interest

If the data transfer does not directly serve the purpose of the employment relationship, justification may be provided based on § 28 (1) sentence 1 No. 2 of the Federal Data Protection Act.

Having recourse to this act does not allow the regulatory framework established by § 32 of the Federal Data Protection Act to be circumvented. Data transfers that would allow other group companies to use data in a way in which the employer would also not be permitted are therefore impermissible.

Moreover, the transfer to a group company must be necessary to safeguard the employer's justified interests. The interests of the affiliated company are, in principle, of no relevance. The employees' interests in having their data stored, only with their employer, must also be taken into consideration. In the view of the supervisory authorities, such interest in principal outweighs the employer's interest in data transfer. This view seems generally too far-reaching. Nonetheless, one will have to adjust to this official practice. The employer will therefore have to take protective measures for the benefit of the employees in order to reach an outcome that is advantageous for the employer. Such measures may include, for example, establishing a group-internal data protection concept in addition to binding regulations between the participating companies.

c) Works Agreement

Data transfer can, ultimately, also be justified based on a works agreement. According to the German Federal Labor Court, they are covered by the statutory provisions of the Federal Data Protection Act (recent Federal Labor Court ruling of 9 July 2013 – 1 ABR 2/13 [A]). This solution may be particularly suited for group structures. In this respect, a separate works agreement concerning data protection is not required. The permissibility of transfer may also result from a works agreement concerning a different subject such as a group-wide incentive system.

II. Additional Requirements for Transmission to a Foreign Country

If the affiliated group company is domiciled abroad, there are stricter requirements to be fulfilled. The data transfer then does not only have to be "per se" permitted. In addition, there must be an adequate level of data protection in the receiving country.

1. EU and EEA

A transfer of data within the European Union and the European Economic Area is not a problem. Data privacy protection laws are largely harmonized within the European Union by way of the Data Protection Directive (EC/1995/46). The European Economic Area contracting countries

Norway, Iceland and Liechtenstein have adopted the EU Directive and also warrant a level of data protection that corresponds to that required under the Federal Data Protection Act. Data transfers to these countries do not, therefore, require any additional justification.

2. Non-Member Countries

Data transfers to recipients outside the European Union and the European Economic Area are permitted only when certain prerequisites are met. "Non-member countries" are generally deemed "unsafe" from the perspective of EU data privacy protection law. A permissible transmission under general data privacy protection rules thus requires supplemental measures to ensure an adequate level of data protection on the "second level" (§ 4 b (2), (3) of the Federal Data Protection Act).

For some countries, the EU Commission has positively determined the required level of protection within the framework of decisions on adequacy. These countries include Andorra, Argentina, Canada, Switzerland, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand and Uruguay.

If the level of data privacy protection is not adequate, the data may be transferred only in exceptional cases (§ 4 c of the Federal Data Protection Act). For example, a transmission based on the consent of the employee (see above) or – but this is interpreted very strictly – a transmission that is necessary to perform a contract is permissible. In addition, the regulatory authorities may approve the transfer as an exception. "Binding corporate rules" that apply with the group may also be approved. It is also possible to achieve an "adequate level of data protection" among group companies by way of contractual agreements.

If certain standard contracts ("EU standard contractual clauses") are used, no additional approval from the regulatory authorities is required, at least in Germany. The EU Commission has made a binding decision with regard to the EU standard contractual clauses that they warrant an "adequate level of data protection". This decision will, however, be reviewed over the mid-term by the European Court of Justice (ECJ).

3. Special Case: USA

The "Safe Harbor" concept used to be a special rule that applied to data transfers to the United States. The recipient companies domiciled there could undertake to provide the "adequate level of data protection" by way of a self-certification procedure. Subsequently, data transfers to these companies were deemed safe in terms of data protection law. The ECJ overturned this option in October 2015 and declared "Safe Harbor" invalid. The background for this decision was ostensibly formal defects, but mainly inadequate protection against government surveillance.

The EU Commission came up with something better in July 2016 and decided on the EU-U.S. Privacy Shield. The "Safe Harbor" successor – like "Safe Harbor" – is based on a self-certification of the data recipient in the United States. The companies must submit to the data privacy protection standards set out in the EU-U.S. Privacy Shield Framework Principles. If they do this, an "adequate level of data protection" is assumed to exist until further notice. It remains to be seen whether the "Privacy Shield" will withstand a court review.

B. Future: EU General Data Protection Regulation

The General Data Protection Regulation will not provide for any group privilege as of May 2018 either. For the first time, however, relevant interests of group companies are explicitly mentioned. According to Recital 78 regarding the General Data Protection Regulation, the interest of a "group of undertakings" in the transmission of data is recognized as a legitimate interest. Although this does not make reviews of individual cases obsolete, the result of a weighing up of interests cannot (any longer) be in favor of the employees from the beginning. It should be possible in the future to bring what currently appears to be a borderline case and requires inconvenient solutions better in line with practical needs. When data are transferred abroad, additional requirements will still have to be met in the future – comparable to the current legal situation.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

FEBRUARY 2017
What Employers should know about the January 27, 2017 Executive Order Concerning Visa Issuance and Travel into the United States
Michael H. Gladstone

NOVEMBER 2016
The Rights of Transgender People – More than a Minor Minority Issue
Cecilia Lahaye

SEPTEMBER 2016
Hively v. Ivy Tech Comty. Coll., S. Bend, 15-1720, 2016 WL 4039703 (7th Cir. July 28, 2016): Sexual Orientation Discrimination not (yet) Covered by Title VII
Eve B. Masinter and Rachael M. Coe

AUGUST 2016
The EU Blue Card
Gerlind Wisskirchen

JUNE 2016
Internet of Things – Work 4.0 – Working When and Where It Is Convenient?
Gerlind Wisskirchen

MAY 2016
Tyson Foods, Inc. v. Bouaphakeo, et al.:
Employees Win on Liability, but Will They Ultimately Bring Home the Bacon?
Eve B. Masinter and Rachael M. Coe

APRIL 2016
What's New in Immigration? A Few Thoughts for 2016
Michael H. Gladstone

MARCH 2016
A Victory for Business Owners in the War of "Employee v. Independent Contractor"
Robert A. Luskin and Erin A. Easley

NOVEMBER 2015
Fifth Circuit Signals to NLRB to Show Respect and Shun Sophistry
Eve B. Masinter and Rachael M. Coe

JUNE 2015
Spotting the Ambush: NLRB's "Quickie" Election Rules
Larry Smith