# Data privacy laws go Europe!

## A new era for employee data privacy compliance under GDPR, DSAnpUG-EU and the EU-US Privacy Shield

By Dr. Daniel Klösel

**Things will be getting serious in 2018!**

In recent years, data privacy matters have become a key management and compliance issue throughout Germany and Europe. This trend was preceded by numerous data privacy affairs involving large and popular companies such as Daimler, Telekom and Deutsche Bahn, to name just a few examples in Germany. As a result of the affairs, these companies were subject to administrative fines totaling up to several million euros and extensive negative press coverage. And not long ago after the European Court of Justice (ECJ) had declared the Safe Harbor Agreement invalid, the German data protection authorities imposed further penalties on certain multinationals, including Unilever, Adobe and Punica, because they had refused to adjust their agreements on data transfers to the US.


The EU lawmakers take data privacy compliance very seriously and so all companies with businesses in Europe should as well!



Under the EU General Data Protection Regulation (GDPR) – which replaces all domestic data privacy laws in Europe as of May 25, 2018 – this situation is getting even more serious. One aspect which materially differs from existing laws is the tightened fine regime GDPR introduces for administrative offenses now drawing fines of up to €20 million or 4% of the total worldwide annual turnover of the preceding financial year. In comparison, the scope of possible fines for data protection violations under existing laws in Germany does not exceed €300,000.

This quite clearly illustrates that the EU legislator takes data privacy compliance very serious and so all companies with businesses in Europe should also do!

→

## Milestones

Data privacy regulation is probably the area of law that has been subject to the most radical change over the last couple of years. And the driving force has been the European Union:

In May 2016, European lawmakers passed the entirely new GDPR, replacing all domestic regulations as of May 25, 2018. Directly applicable without any further need for domestic legislatures to formally adopt it, GDPR provides for almost 100 provisions on data privacy and generally tightens the current laws of many EU member states. There are certain doubts, however, whether GDPR will also lead to a uniform level of data protection in Europe as it allows the member states to introduce national laws in order to implement the EU regulation. As a result, the German government had already presented a draft legislation *(DSAnpUG-EU)* in February 2017 which shall become effective still this year. The legislation provides for supplemental rules in particular on employee data privacy mostly in accordance with the current laws in Germany.

Only a few months before in October 2015, during the decisive phase of the GDPR negotiations, another milestone on data privacy issues has been achieved as the ECJ declared the existing Safe Harbor arrangement to be void. As a consequence, many multinationals with businesses in Europe – which either transferred data to their parent companies located in the US and/or made use of US-based IT (cloud) services had to adjust their contractual arrangements mostly by relying on EU model clauses. After the EU and the US government agreed on the EU-US Privacy Shield as successor agreement to Safe Harbor in 2016, a few multinationals have also made use of this new solution yet and initiated the necessary self-certification procedure.

## "Two levels of justification"

Presenting all the impacts of these new laws is hardly possible here. Nevertheless, the general concept of the European data privacy regime could be summarized with "two levels of justification" which is also similar to the existing German model.

On a first level, in any case personally identifiable data may be processed if and to the extent that applicable laws provides for a legal basis (art. 6 para. 1). Under GDPR and the supplemental German rules three opportunities remain significantly relevant in practice:

- At first, an individual consent of the affected employees which is, however, only valid under GDPR in case it has been granted voluntarily and meets further requirements. These pertain, in particular, to the style of the consent form: It must be intelligible and easily accessible as well as written clearly and in a plain language (Article 6, paragraph 1 (a), 7). In addition, the German draft laws provide for even stricter specifications: Consent is only regarded as being voluntarily when it is based on legal or economic advantages for an employee or on the equal interests of both, the employer and the employee. Moreover, consent has to be issued in writing and certain additional obligations concerning the employee's right to withdraw consent as well as the purposes for processing the data covered by the consent have to be provided (Article 26, paragraph 2).

- The GDPR also provides for additional legal justifications including, but not limited to, the prevailing interests of the company as part of a comprehensive assessment and as related to compliance concerns for purposes of preventing and investigating criminal acts (e.g., Article 6, paragraph 1 [f]). The supplemental German rules then provide for more precise definitions for the cases in which data processing is "appropriate" and therefore legally justified on this basis (Article 26, paragraph 1).

- Furthermore, and this is of great significance for employee data protection matters, works agreements between a company and its works councils continue to constitute a sufficient legal basis. Similar to the practice of German courts, such works agreements must, however, comply with the applicable data protection regulation, in particular now with the GDPR (Article 82, paragraph 1 of the GDPR and Article 26, paragraph 4 *DSAnpUG-EU)*.

The second level relates to cases where data is to be transferred outside the EU. Here, additional legal justification must cover foreign data transfers. Under the GDPR, such a legal basis may also be provided by individual consent that then has to meet further requirements, in particular requirements related to information addressing the possible risks to the subject of the data if such transfers are made (Article 49, paragraph 1).

As consent pertaining to either level may be withdrawn by an employee →

at any time (Article 7, paragraph 3), GDPR provides for alternative solutions on the second level as well. These solutions are based either on an "adequacy decision" (Article 45) or other "appropriate safeguards" such as EU model clauses or binding corporate rules (Article 46). At present, data transfers to the US in particular are generally privileged by such an adequacy decision due to the Privacy Shield Agreement. The German supplemental rules only provide for some clarifications on this situation (Article 78 et seq.).

## Further changes, but no intragroup privilege!

Aside from this general concept, GDPR provides for additional changes in terms of its extraterritorial applicability, in particular to any data processing related to business activities with a company's establishment in the EU regardless of whether it takes place in the EU or not (Article 3, paragraph 1; further extensions are stipulated in Article 3, paragraph 2). Other substantial changes comprise the appointment and the role of data protection officers (Article 37 et seq.) as well as significantly extended documentary obligations for companies in conjunction with further information rights of employees (Article 12 et seq.).

Furthermore, GDPR still provides for the general privilege of processing data on behalf of the controller (Article 24 et seq.). If this privileged model remains particularly significant in practice – either with regard to data transfers within multinational groups or when using external IT (cloud) services – the GDPR also stipulates extended obligations for data controllers and, especially, for data processors (Article 30).

However, another privilege that is significantly important in practice could not be established: the intragroup privilege where a group division would not be deemed as third party similar to the privileged status reserved for processing data on behalf of the controller. Even if rec. No. 48 refers to the potential interest of multinational groups to transfer data between single entities (which certainly goes in the right direction), the requirements for justification mentioned above remain generally applicable to these cases as well.

## Substantial impacts: adjustments of contracts and the like

These new European laws pose a major challenge for complying with data privacy. This particularly applies to any existing agreements: Consent declarations, works agreements and intercompany agreements with affiliated companies and external providers need to be reviewed and adjusted with respect to the tightened requirements under the new European data privacy laws as well as the German supplemental rules.

Aside from tackling this legal paperwork, several additional steps may also have to be taken, for example, reviewing the IT environment to determine whether it provides the necessary technical infrastructure to fulfill the extended documentary and information obligations. But the new laws do not just provide for extended obligations, but also alternative solutions like the EU-US Privacy Shield. These do, of course, require that certain additional measures be implemented, particularly self-certification in the US.

## May 25, 2018: The clock is ticking!

All these necessary adjustments have to be finalized before GDPR takes effect on May 25, 2018. At first glance, this timeframe does not appear very challenging, but it is. As the necessary adjustments will often require negotiating with works councils, affiliated companies and/or other third parties like external IT providers, companies have no time to waste to ensure their compliance with data privacy under the new European laws. The increased fines of up to €20 million or 4% of a company's total worldwide annual revenue may not be the only reason to justify such effort, but certainly is a very important one! <–

**Dr. Daniel Klösel**
Rechtsanwalt
JUSTEM Rechtsanwälte, Frankfurt am Main

*d.kloesel@justem.de*

**www.justem.de**