POSITION PAPER

Berlin, 2 July 2019

Deutscher Industrie- und Handelskammertag e.V. (Association of German Chambers of Commerce and Industry; DIHK e.V.)

Evaluation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)

Who we are:

The Association of German Chambers of Commerce and Industry (DIHK e.V.) is the umbrella organisation of the 79 Chambers of Commerce and Industry (IHKs) in Germany. Our common goal: Best conditions for successful business.

In Germany and in Europe, DIHK represents the collective interest of German business towards policymakers, administration and the public.

Several million commercial, industrial and services businesses are members of a Chamber of Commerce and Industry by law – from kiosk owners to DAX-listed corporate groups. DIHK and IHKs are consequently a platform for the diverse interests of business. We combine these interests in an established procedure with a statutory basis in order to present common positions of German business and contribute to economic policy opinion-forming.

DIHK also coordinates the Worldwide Network of 140 German Chambers of Commerce (AHKs), Delegations, and Representative Offices of German business in 92 countries.

The DIHK is registered in the European Commission transparency register (No. 22400601191-42).

Representation of the Association of German Chambers of Commerce and Industry (Deutscher Industrie- und Handelskammertag e.V.; DIHK) at the European Union
B19 A-D, Avenue des Arts | B-1000 Bruxelles
Tel. +32 2 286-1611 | Fax +32 2 286-1605 | Website: http://www.dihk.de

I. Background

According to Article 97 of the Regulation (GDPR), the European Commission must submit a report "on the evaluation and review of this Regulation" to the European Parliament in 2020. With this position paper, the Association of German Chambers of Commerce and Industry (DIHK e.V.) wishes to participate in the discussion on the Regulation's implementation. For this purpose, with the support of the Chambers of Commerce and Industry (IHKs), it has conducted a survey of some 4,500 companies of all sectors and sizes. In terms of the size of their workforce, more than 80% of those companies were SMEs as defined by the European Commission. However, companies with from 250 to over 1,000 employees also responded to the survey.

II. Demands

Based on our survey findings, the Commission should consider the following points in its evaluation of the GDPR:

- The original objective of harmonisation and unification of law should be pursued more intensively. The opening clauses (derogations) lead in practice to a fragmentation of the law that in turn creates diverging market conditions for companies across the EU. Notable examples in Germany include the rules governing designation of a company data protection officer and employee data protection.
- There is an enormous desire for legal certainty. Businesses are worried about receiving legal warnings. Legal uncertainty could be avoided among other things with binding specimen documents and contracts. Uniform guidelines from supervisory authorities can also provide greater legal certainty. There is a general desire for uniform interpretation of the law, including interpretation provided by the supervisory authorities.
- SMEs urgently need facilitations such as simplified rules or exemptions because implementing the GDPR places a disproportionate burden on them. Recital 13 should be understood as a mandate for legislative action.
- The documentation and verification obligations are generally considered too strict and disproportionate. Facilitations could be provided here in cases where, for example, processing of data is not the main focus of a company's business. It is therefore proposed that the entire B2B sector should be provided with facilitations under Article 12 et seqq. GDPR.
- A further point of criticism is the lack of privileged treatment for group companies. Privileged treatment should be provided for companies within a corporate group.
- The experience gained with implementation of the GDPR should be taken into account in the legislative process for the ePrivacy Regulation.

Representation of the Association of German Chambers of Commerce and Industry (Deutscher Industrie- und Handelskammertag e.V.; DIHK) at the European Union
B19 A-D, Avenue des Arts | B-1000 Bruxelles
Tel. +32 2 286-1611 | Fax +32 2 286-1605 | Website: http://www.dihk.de

- Legal requirements that companies can only implement at great expense in terms of financial and human resources reduce acceptance of the rules and ultimately miss their mark. A case in point is the requirement of consent as the all-pervading legal basis of the ePrivacy Regulation.
- As there is reason to fear that the ePrivacy Regulation will have similar consequences in practical implementation as the GDPR, the ePrivacy Regulation should take greater account of the needs of SMEs and the reality they face, and should provide facilitations and exemptions for them.
- The legislation must be accompanied by explanatory and advisory measures so that SMEs are also able to implement the rules. This applies in particular to technical implementation.
- The ePrivacy Regulation and the GDPR should be consistent and coherent.

III. General

Data protection is a fundamental right under Article 16 TFEU. The EU is therefore under obligation to flesh out that right. It fulfilled that obligation by adopting the Regulation.

In view of the rapidly advancing digitalisation of private and public life, data protection is a fundamental and important element of the European Single Market. The global nature of data flows means that data protection can no longer be governed by individual nation states and an international framework is needed instead. However, the GDPR can be no more than one small step towards such an international framework.

Until binding international agreements are in place, the EU must be quicker in adopting adequacy decisions than has so far been the case. Adequacy decisions must also be long-lasting and robust, but this is questionable in the case of the Privacy Shield.

If the United Kingdom exits the EU without agreement on the continued application of the GDPR, then not too much should be expected of a corresponding adequacy decision if the EU is in the process of deciding on an E-Evidence Regulation at the same time.

It remains questionable whether the GDPR is sufficiently future-oriented and can meet needs such as those created by artificial intelligence.

IV. Effects of the Regulation's entry into force

Implementation of the GDPR was already a topic of discussion after its entry into force on 24 May 2016. Issues surrounding the GDPR became an increasing focus for companies in late 2017 and early 2018 as the 25 May 2018 application date drew near. This was the same for companies of all sizes and sectors. The Chambers of Commerce and Industry registered a considerable need among companies for information and advice.

Representation of the Association of German Chambers of Commerce and Industry (Deutscher Industrie- und Handelskammertag e.V.; DIHK) at the European Union
B19 A-D, Avenue des Arts | B-1000 Bruxelles
Tel. +32 2 286-1611 | Fax +32 2 286-1605 | Website: http://www.dihk.de

Numerous events were held to provide general information on the requirements under the GDPR and also to advise on specific implementation steps. A roadshow supported by the Federal Ministry for Economic Affairs and Energy also helped ensure that companies were informed. It emerged that even larger companies, and especially those operating across borders, needed to devote considerable human and financial resources to implementing the GDPR. Small and medium-sized enterprises have problems implementing the GDPR to this day because they lack the necessary expertise and there is a shortage of knowledgeable consultants. The data protection supervisory authorities are also unable to meet the need for advice.

A further and related problem is legal uncertainty due to the GDPR's openness to interpretation. On the one hand, this provides companies with latitude in how they approach implementation in practice. On the other, however, it transpires that data protection supervisory authorities, courts and consultants come to different conclusions on matters such as joint controllership. This exacerbates the confusion among companies and their fear of sanctions from the supervisory authorities.

V. Objectives of the GDPR

1. Harmonisation

One of the most important arguments in favour of creating the GDPR was the full harmonisation of data protection law in the EU – in principle an approach that is to be supported. This is also confirmed by the survey findings. The opening clauses (derogations), however, provide the Member States with latitude for national rules, and this can lead to gold plating – as seen with employee data protection. In addition, the supervisory authorities in the Member States have free rein in their interpretation of the GDPR when making decisions within the national framework, resulting in diverging procedures between Member States.
The European Data Protection Board (EDPB) will not be able to find an EU-wide interpretation for every eventuality. In addition, the EDPB is required to base its decisions on the lowest common denominator.

The supervisory authorities in the Member States also differ in the human and material resources available to them, which in itself can result in differences in law enforcement.

It is therefore to be hoped that the consistency mechanism will lead to greater unification of legal opinions.

The survey shows that nearly a third of respondents take a positive view of the opening clauses in the GDPR; however, about half of the companies surveyed do not consider themselves to be affected by them. Companies with a negative view of the opening clauses are critical regarding the risk of fragmentation of the law and the resulting competitive disadvantage (distortion of competition) due to the generally stricter rules in Germany.
The consequences are greater effort and expense in order, for example, to keep abreast of and comply with the national rules; this relates to matters such as designation of a suitable data protection officer or the rules on employee data protection. Diverging interpretations of the law and differences in approach/rigour between supervisory authorities are also viewed as disadvantages,

however. A majority of companies with experience of data protection rules in other EU Member States indicated that the rules there are less strict.
The desire for harmonisation of the law and a uniform legal framework across the EU is very pronounced among the companies surveyed. This is because additional rules on top of the GDPR increase legal uncertainty and the regulatory burden for companies operating across borders.

2. Marketplace principle

The marketplace principle is welcomed by large companies as creating a level playing field. The possibilities for obliging large companies from third countries to comply with the GDPR nevertheless present a challenge. This needs to be addressed in the near future at European level to avert the impression that only SMEs are subject to sanctions.

3. Balance of interests between citizens and business

The GDPR has two aspects: Protection of EU citizens' private sphere versus free movement of data, meaning the ability for companies to process data and use it across borders. The conflict of interests between the business use of data and its protection has been resolved in the GDPR in a way that tips the scales in citizens' favour. Applications such as big data or involving artificial intelligence pose considerable difficulties in particular for companies whose business model relates solely to the processing of data.
The survey shows that regardless of workforce size, the majority of respondents consider data protection an important issue for their company.

4. Risk-based approach

The GDPR applies a risk-based approach, meaning a flexible response to prevailing data protection needs. A positive aspect is the stronger linkage made between data protection and information security. The risk-based approach is not applied consistently throughout, however. Thus, only in Article 37 is a management responsibility such as the appointment of a company data protection officer made dependent on whether data processing is among the company's "core activities". Everywhere else, a one-size-fits-all approach is applied. This neither reflects corporate reality, nor does it improve data protection. All other obligations apply regardless of company size or business model. The risk-based approach fails to help improve data protection as numerous bureaucratic obligations – such as the obligations to provide information under Articles 13 and 14 – continue to apply even when a contractual relationship is involved and both parties already know what data is processed and for what purpose.

Representation of the Association of German Chambers of Commerce and Industry (Deutscher Industrie- und Handelskammertag e.V.; DIHK) at the European Union
B19 A-D, Avenue des Arts | B-1000 Bruxelles
Tel. +32 2 286-1611 | Fax +32 2 286-1605 | Website: http://www.dihk.de

VI. Effects on corporate reality

1. Positive and negative aspects

The survey shows that the larger a company, the more positive aspects are identified. The GDPR creates greater transparency for the processing of personal data. Its entry into force was taken as an opportunity to review, optimise and professionalise internal processes and structures. Companies minimised and purged their holdings of data and standardised their processes. The GDPR also resulted in greater awareness of and sensitisation to data protection among employees and management, but also among customers. The stronger linkage made between data protection and data security is likewise regarded positively.

However, over half of the companies surveyed did not see any positive aspects for their business. Many companies recognise the importance of well-functioning data protection but consider the GDPR to be overshooting the mark. In particular, the great majority (nearly 90%) of companies surveyed criticised the enormous increase in red tape occasioned by the GDPR while about 70% reported a large to very large commitment of financial resources and about 60% a large to very large commitment of human resources.

The greatest effort and expense was incurred for compilation of the record of processing activities, the information obligations/data protection notice, the technical and organisational measures, and processing. Respondents also cited the introduction of a data protection management system, and in particular the development and implementation of a deletion policy, and, in the case of larger companies, international data transfer.
A further point of criticism was the short time limit for reporting data breaches, which in practice is hard to comply with.

Companies already face large volumes of right-of-access requests. This matter becomes especially relevant in cases such as where a former employee asks for the surrender of specific emails or a member of staff demands to be provided with all internal corporate communication.

2. Effects on business activities

A number of companies indicated that they had scaled back or even discontinued business models due to the increased requirements, and also due to the attendant legal uncertainty and the resulting risk of legal warnings. This primarily related to the areas of photography, advertising, web/social media marketing and data-driven business models in general, such as in healthcare. There are even cases in which the use of email for purposes such as advertising has been abandoned.

3. Response from customers and trading partners

The GDPR has been lauded among other things for giving EU companies a competitive advantage over competitors. For it to have that effect, however, data protection has to be regarded positively by customers and trading partners. Yet according to the survey, 70% of respondents do not see it as providing a competitive advantage or image enhancement. In particular, customers frequently complain of information overload.

Usability of communication (e.g. WhatsApp) is frequently more important to them.

4. Special situation of small and medium-sized enterprises

Micro, small and medium-sized enterprises experience the implementation of the GDPR as being even more burdensome for them than for larger companies. They do not have the staff to look after implementation, and outside consultants are expensive or even unavailable. As consultations by the Chambers of Commerce and Industry have already shown, and as confirmed by the survey, SMEs consequently have a strong interest in specimen documents, guidelines, checklists and standard requirements that they can adapt to their own corporate reality (if they adapt them at all) so as to be sure of complying with the rules.

Aside from practical support in implementation, however, SMEs in general demand reliefs from the legal obligations. The exemption for SMEs in Article 30(5) effectively does not apply in practice. The GDPR does not deliver on the objective expressed in Recital 13 of taking into account "the specific situation of micro, small and medium-sized enterprises". The possibility should therefore be examined, for example, of supplementing the criteria for imposing administrative fines under Article 83 GDPR by expressly adding SMEs to Article 83(2).
SMEs also hope for facilitations with regard to compilation of the record of processing activities and the information obligations. These should be graduated according to business model, for example with small industrial companies that do not have end consumers among their customers to be exempted from the information obligations on the basis of the risk-based approach.

Contact:

Annette Karstedt-Meierrieks
Legal Department
Director
Administrative Law,
Public Procurement, Data Protection

DIHK – Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29, 10178 Berlin
Tel.: +49-30 20308-2706
Fax: +49-30 20308-5-2706
mailto: karstedt-meierrieks.annette@dihk.de
http://www.dihk.de

Kei-Lin Ting-Winarto
Legal Department
Director Data Protection

DIHK - Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29, 10178 Berlin
Tel.: +49-30 20308-2717
Fax: +49-30 20308-5-2717
mailto: ting-winarto.kei-lin@dihk.de
http://www.dihk.de