MEMMINGER LLP

The EU General Data Protection Regulation will go live on 25 May 2018 – high time to get your company ready for a new era of data protection

November 2017

The EU General Data Protection Regulation (GDPR) of the European Parliament and Counsel is getting serious soon. From May 25, 2018, it will be binding in all EU member states without the need for an act of transposition – as in the case of a directive – into the respective national law. The GDPR has already been in force since May 2016. However, it provides for a two-year grace period in which data controllers and other norm addressees are given the opportunity to align their processes, systems and clauses with the new data protection calendar. The length of the transitional period may serve as an indicator of the complexity of the measures that legislators are expecting the companies to take on. After 2/3 of the transitional period has already passed, the pressure to act is currently increasing dramatically in many companies. It is necessary to say goodbye to the idea of adopting, if necessary, the solution of another market participant who has taken action in a timely manner. A "one fits all" solution does not exist because the nature and extent of the necessary measures depend on the specific circumstances of each company.

I. Purpose of this Urgent Reminder

The upcoming activation of the GDPR means that there is extensive action needed in many companies. This can range from technical changes (privacy by design) to the renegotiation of company agreements.

This paper should sensitize the decision-makers to the fact that in principle no day may be wasted, if one does not want to risk grave breaches of compliance. At the same time, it wants to guard against blind actionism; there is still no cause for panic for most market participants (which would be fully justified if particularly highly-exposed companies like Google, eBay or Amazon would only start to worry now). We are happy to help you arrive at timely, legally compliant solutions with a clearly structured approach.

II. What are the essential adjustments that are required?

1. There are significantly more stringent documentation requirements with regards to the planning and implementation of data processing in order to facilitate the proof of data protection compliance vis-à-vis the supervisory authorities.

2. **Data protection policies** must comply with considerably expanded information obligations which in most cases will probably not exist yet.

3. The formal requirements for **declarations of consent**, in particular the documentation requirements regarding the voluntary nature of consent, were sharpened; an established process for the revocation of consent is now mandatory.

4. Existing company agreements in many cases no longer fit the requirements of the GDPR. It can take a long time to reach an agreement with the employee representatives on the resulting need for change with regard to some of the already existing company agreements.

5. Standard clauses for contract data processing in any case require an adaptation to the new rules on the joint and several liability of the contract data processor and their own documentation requirements, which will exist in addition to those of the data controller.

6. The processes for dealing with **data breaches** also need to be redefined, such as compliance with the 72-hour deadline, required in certain cases, to inform the

supervisory authorities and the parties concerned.

7. Data privacy risks can best be minimized if employees have internalized the essential importance of this area and the dangers to which it is exposed. This can best be achieved by sensitizing employees through target group-specific training and other "awareness measures".

8. In many cases, a formalized risk assessment to determine the necessary and appropriate technical and organizational measures for the protection of personal data, as required by the GDPR in the future, will not even exist in the first place.

9. This applies in particular to the newly introduced requirements for audit standards and documentation requirements for the future data protection impact assessment. They are required as part of data protection risk management.

10. Considering the complex interplay of European and national legislative acts, active monitoring of legislative activities at all levels is currently required, for example with regard to a further specifications of employee data protection or the competences and related obligations of the Data Protection Officer. They are part of the standard repertoire of the responsible departments to counteract as early as possible with corresponding organizational / technical measures.

III. Conclusion

That a proper implementation of the above catalogue is not child's play, should be general consensus. Combined with a drastic increase in the fine for certain compliance violations of up to 20 million or 4 % of worldwide annual sales, will bring exciting weeks in the time to come. Face the challenge!

MEMMINGER LLP

Memminger LLP
Bleichstraße 64-66
60313 Frankfurt am Main

+49 (0) 69 870 047 800
info@memmingerllp.com
www.memmingerllp.com

Contact:
Prof. Dr. Wolfgang G. Büchner
Benjamin Schütze