First Lessons Learned

Nine Months EU General Data Protection Regulation

By Dr. Michaela Nebel

The EU General Data Protection Regulation ("GDPR") which became applicable on May 25, 2018 received a lot of attention in the media and increased the awareness of data protection in the population at large. It also caused significant efforts for companies to implement appropriate compliance steps. On January 25, 2019 the European Commission published a statement on the GDPR, summarizing the effect of the new data protection rules positively. The statement provides a good occasion for a review of the first nine months of the GDPR and lessons learned.

Significant increase of complaints

Since the GDPR became applicable, complaints with the local data protection authorities have increased significantly. Pursuant to Art. 77 GDPR every data subject has the right to lodge a complaint with a data protection authority if the data subject considers that the processing of personal data relating to him or her infringes the GDPR. The European Commission published interesting →

Data protection has become a large compliance risk area.

figures in this regard: Since May 25, 2019 local data protection authorities received more than 95,000 complaints from citizens lodged by individuals or by organizations mandated by individuals. According to the European Commission the most common reason for complaints are related to telemarketing, direct marketing emails and video surveillance. While the volume of the complaints is new, the reasons for the complaints are well-known and have already led to complaints before the GDPR entered into application.

Significant increase of breach notifications

Under the GDPR, the requirements when to notify a personal data breach to the data protection authority, have been lowered. First of all, the definition of "personal data breach" is quite broad since it covers every breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Furthermore, personal data breaches must be notified to the data protection authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In addition to that, personal data breaches must be notified to the data protection authority without undue delay, and where feasible, not later than 72 hours after having become aware of it. Correspondingly, the amount of personal data breaches has increased. According to the European Commission companies notified more than 41,000 personal data breaches to their local data protection authorities since the GDPR came into application. Due to the high fines that could be imposed in case of non-compliance with a notification requirement, companies tend to notify even if there is no notification requirement and in particular in case of doubt.

>>
But also the first administrative fines were imposed.
<<

First enforcement actions

The GDPR provides the data protection authorities with a variety of investigative and corrective powers, including to impose administrative fines up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. A few months after the GDPR became applicable, the first enforcement actions from the local data protection authorities were published.

The data protection authorities for the German states of Lower Saxony and Bavaria are carrying out random audits to check compliance with the GDPR. For example, the Bavarian data protection authority audited websites with a wide coverage and found that the results were rather disappointing: There were plenty of deficiencies regarding the protection of passwords by online service providers and the use of tracking tools on websites.

But also the first administrative fines were imposed. In Germany the data protection authority in the state of Baden-Wuerttemberg imposed a fine of € 20,000 on a chat platform provider for violating its obligation to ensure data security. As part of a data breach notification to the data protection authority following a hacker attack whereby personal data (including passwords and email addresses) of approx. 330,000 users were stolen and then made publicly available, the provider itself revealed that the customers' passwords were stored in an unencrypted manner. For its decision on the amount of the administrative fine, the data protection authority considered in particular that the provider fully cooperated and promptly followed the data protection authority's recommendations. But also the Austrian data protection authority imposed a first fine: The Austrian data protection authority imposed a fine of around EUR 5,000 against an entrepreneur for having installed a CCTV camera in front of his establishment, also recording a significant part of the side walk and not having properly informed about it. Also the data protection authority in the United Kingdom - the ICO - imposed several fines and issued warning letters - many of them in connection with unsolicited direct marketing activities. The French data protection authority - the CNIL - issued the highest fine so far - EUR 50 million for lack of consent and transparency.

It remains to be seen how enforcement activities develop and whether the data protection authorities in the EU Member States align on the amount of fines.

Adaption of national data protection laws

Although the GDPR as an EU regulation applies directly in all EU Member States (i.e. without a further implementation by the EU Member States) the GDPR contains more than 50 so-called open- –>

ing clauses that require and allow the EU Member States to implement national data protection laws which supplement the GDPR. In particular, the GDPR allows for deviations among the Member States regarding the following topics: (i) How old must a minor be to validly consent to the processing of his/her personal data? (ii) When is it not possible to consent to the processing of sensitive data? (iii) Is the processing of genetic data, biometric data of health data subject to additional limitations? (iv) Are the rights of the data subjects subject to additional limitations? (v) Do all controllers and processors have to appoint a data protection officer or only certain controllers or processors? As of January 2019, 23 out of 28 EU Member States adopted national data protection laws supplementing the GDPR, whereas five countries are still in the process of doing so (Bulgaria, Greece, Slovenia, Portugal, Czech Republic). Whereas some countries made as few changes as possible to their existing data protection laws and implemented only mandatory opening clauses (e.g. Austria) other countries made more extensive use of the opening clauses (e.g. Germany).

Guidelines published

The European Data Protection Board, responsible for ensuring the consistent application of the GDPR, published a number of guidelines and other documents on various aspects of the GDPR in order to provide guidance regarding the interpretation of the GDPR and to contribute to a consistent application of the GDPR. The European Data Protection Board also endorsed a number of guidelines published by its predecessor, the Art. 29 Working Party, e.g. the guidelines on consent and transparency. Also the national data protection authorities have been quite active in publishing guidelines and papers on the interpretation of the GDPR.

Summary

It remains to be seen how the GDPR and the supplementing national data protection laws, in particular their interpretation by the data protection authorities and by the courts turn out in practice. However, the first few months of the GDPR show that companies must take the GDPR seriously. Data protection has become a large compliance risk area. Thus, companies are well advised to implement a proper data protection compliance program, if not done so yet, and to constantly work on it.

Editor's note:
Michaela Nebel (born Weigl) is one of the authors of the book Feiler/Forgó/Weigel, The EU General Data Protection Regulation (GDPR) – A Commentary. The book is published in association of www.globelawandbusiness.com and www.germanlawpublishers.com. You will find the details here: https://www.globelawandbusiness.com/books/the-eu-general-data-protection-regulation-gdpr-a-commentary. (tw) <–

Dr. Michaela Nebel
Rechtsanwältin, Partnerin,
BakerMcKenzie, Frankfurt am Main

Michaela.Nebel@bakermckenzie.com

www.bakermckenzie.com