How GDPR affects business in SEE

by Maya Aleksandrova,
Attorney-at-law/Senior Associate
CMS Reich-Rohrwig Hainz

The General Data Protection Regulation (GDPR) was approved in 2016 but went into effect as of May 25, 2018, as it repealed and replaced the previously existing EU legal data protection framework. The main prerogative of the new data regime is the establishment of more rights for private individuals, the demonstration of transparency and the levy of more robust rules for enforcement in case of non-compliance with the legislation.

The most important obligations that the GDPR establishes and develops for all businesses in the EU include the following: update of privacy policies and notices; update of the relevant declarations of consent; maintain records of data processing activities; review and amendment of the relevant website content and policies; adapting the provisions of commercial and employment agreements; improvement of the legal grounds for data transfers; establishment of stricter procedures for notification of the individuals and the competent authorities in case of security breach. In certain cases, the companies are required to carry out a data protection impact assessment for particular data processing operations and to appoint a data protection officer/representative in the EU.

The abovementioned obligations lead to considerable administrative and organisational efforts and changes for the companies, including spending a substantial budget for adopting policies, performing of staff training and concluding the necessary agreements; undertaking the appropriate technical and organisational measures; creating new jobs and extending security/data protection staff; coordinating the internal efforts with external legal and IT consultants; undertaking actions to secure cross-border data transfers within and outside the corporate group, etc.

In practice, the first mass awareness wave about the new data regime came for the SEE companies in the autumn of 2017. By this time, only the major players such as some of the banks, insurers, telecoms, etc., had commenced preparing for the new data rules. The businesses needed time to be acquainted with the changes that GDPR requires, determine a budget and appoint team members to handle the GDPR implementation. In many cases, companies are still undergoing the exercise of becoming fully compliant with the new data protection rules.

Although under the GDPR there are some requirements that are carved-out for small companies, most obligations apply to all enterprises irrespective of their size and activities. Since it entered into force, the GDPR has affected the different-sized businesses in the SEE region in an exceptionally ambiguous way, as the economic segmentation of the companies in this part of Europe encompasses a variety of entities (i.e. large international corporations, institutional investors, local SME's, as well as one-man companies), and there is a vast financial and organisational gap between them.

Another significant issue comes from the fact that some countries in the SEE region are EU members, while others are not. In this regard, there are specifics in the way that the GDPR affects the business in the SEE region.

> One-third of local companies in EU member states in SEE tried to show GDPR compliance by May 2018.

For the businesses domiciled in EU member states the situation is straightforward – they fall under the GDPR's terms and are obliged to follow the requirements of the new regulation. These businesses have to modify the way they collect, process and store personal data. However, and more importantly, the GDPR applies extraterritorially – not just to organisations within the EU, but also to businesses who offer goods or services to individuals in the EU, or monitor the behavior of individuals in the EU. For the companies in countries outside the EU, this means that they are required to apply one set of rules when they process data of individuals outside the EU and another set of rules when they process data of individuals located in the EU. Moving forward, these differences in the data processing regime and requirements in the various SEE countries in and outside the EU should be taken into consideration by the foreign investors outside the European bloc, which plan to do business from another part of the world into countries in the SEE region.

In addition, there is a special requirement for the businesses outside the EU (which fall under the GDPR regime) to appoint a representative in one of the member states, where are the data subjects, whose data is being processed (i) in relation to the offering of good or services, or (ii) for the monitoring of their behavior. The purpose of such representative is to act as a point of contact with the data protection authority in the respective country, where the data subjects are located. Affected companies would be exempt from this obligation only to the

extent that the data processing happens occasionally and does not include large scale processing of the so-called "sensitive data", and is therefore unlikely to result in a risk for the rights and freedoms of the respective individuals.

Currently, there is no official information on the percentage of the SEE companies that are aware of the new rules. In reality, most of the companies, which began implementing the new data rules, commenced their preparation one or two months before the GDPR's application, in the spring of 2018. We had a bunch of clients' requests in the first half of May, asking for immediate assistance before May 25, 2018. As the GDPR implementation process is a complex procedure, which requires coordinated legal, administrative and IT efforts from the business, very small number of companies in the SEE region succeeded in reviewing and redrafting their policies, and concluding the necessary data processing agreements and supporting GDPR documentation by May 25, 2018. Based on information from unofficial public sources, about one third of the SEE companies located in the EU have tried to show compliance by the GDPR's implementation date. The percentage is even smaller for the non-EU member SEE countries.

Some companies are still working on the implementation of the new rules and have taken the approach to cover first the "visual" issues such as privacy policies, notices and agreements, and to complete the entire process at a later stage. At one end of the spectrum there are companies which are aware of the new regulation, but do not understand that it concerns them, and there are even companies that have not heard of it at all. Based on our experience, the percentage of companies in the latter group is significantly higher in the SEE countries outside the EU than those in the EU.

In line with the trend in the rest of the EU, the new data regime impacts most significantly business sectors in the SEE like banking, insurance, telecommunication, media, marketing, healthcare, etc., which process personal data on a large scale and/or special categories personal data, the so-called "sensitive" data. Most of these companies have undertaken substantial efforts and ensured a considerable budget to prepare for the GDPR. In particular, the multinational companies are more aware of their responsibilities, and therefore have taken structured measures for their subsidiaries in both the EU and non-EU SEE countries. Consequently, the multinational companies often prefer to appoint a data protection officer at a group level, whereas this person is responsible for keeping in line the privacy of the entire corporate group.

As expected, larger companies in the region are more proactive and diligent in terms of GDPR and have taken more efforts to challenge the GDPR implementation than the small and medium-sized SEE companies. One of the reasons for this are the large-scale fines, which may reach up to 20 million euro or 4% of a company's worldwide turnover for the last financial year (whichever number is higher). On the contrary, the approach of many of the small and medium sized companies is to wait for clear-cut instructions from the local regulators and standard forms of documents to complete. There is a general lack of understanding among the latter of the exact meaning of the "personal data" definition and still there are companies claiming that they do not process any personal data, whilst having employees and contracting other parties.

Even though the GDPR has a general application, in practice the local data protection authorities are required to amend and adopt the local acts on the GDPR and to develop the general rules of the regulation. The adjustment of the local laws in the different countries in the region raises a lot of questions and concerns for the companies in the SEE region. Some countries like Croatia succeeded in adopting their legal acts for implementing the GDPR provisions by May 2018. Others like Romania adopted their local legislation soon thereafter. There are others as Bulgaria, who are still working on their local acts and the changes in the legislation are still anticipated. Although the local authorities in the most of the countries issued extensive materials giving interpretations of the GDPR before the time of its application, and there are ongoing training sessions, there is still a large number of companies, which have not established their role and obligations under the GDPR. The prolonged legislative processes, which are still running in most SEE countries, is also another reason for postponing the completion or for some companies even the start of the implementation process.

In conclusion, if your business has not prepared for the new data protection regulations yet, you should reconsider your strategy and develop a plan for compliance with the GDPR.

The present article is not intended to be a comprehensive guidance on the GDPR and the respective data protection rules, but rather an informative piece showing the authors' comments on the impact of the new data regime over the companies in the SEE region.