Applying General Data Protection Regulation (1/44/18)

Since the General Data Protection Regulation (GDPR) came into force on 25 May 2018, data processors have seen its restrictions becoming tighter. What is the difference between protecting personal data and monitoring individuals? And how can the Anti-Money Laundering Directive (AMLD) coexist peacefully with the GDPR?

The GDPR[1] was adopted in May 2018 to improve the EU legislation on personal data. Users now have more statutory rights, and companies breaching them are threatened with a fine of up to €20 million or 4% of annual revenue.

Directives and regulations usually explain how they are interrelated. In the case of a directive, implementing a regulation may cause more difficulties. And these rules are enforced by national statute law and case law. There should be no conflict in general, but companies often cite privacy as the reason for providing inferior services or committing AML breaches.

It is important to remember that the AMLD is a directive but the GDPR is a regulation. There is a crucial difference between the two levels of legislation.

Member states are to pass the AMLD's basic requirements into their national law, but this does not prevent a member state from adopting tighter requirements.

On the other hand, the GDPR is directly and uniformly applicable across the EU, and member states cannot make even small modifications, meaning that data protection in Latvia will be similar to data protection in Germany or France.

Let us look at an example that is often misleading and makes us reconsider how regulations and directives are interrelated: introducing registers of beneficial owners, or rather, the requirement for such registers to be public.

To mitigate the risk of money laundering, it is important to identify the company's real owner, i.e. the person who has a controlling interest in it or otherwise controls its management. This aspect has been invoked by the European Commission in its initiative of 2015 to create national registers of beneficial owners, with such information being transferred to a single European register. And persons who directly or indirectly own more than 25% of the company's share capital and have a certain ability to influence the company's operations, including top management, should be recognised as beneficial owners. A member state has discretion to lower this threshold according to its national law. A centralised register is based on the "Know Your Customer" principle, international standards, and best practice.

So theoretically, information on beneficial owners could be available to everyone. Proposals for amending the AMLD provide that member states should restrict access to information stored on their national registers of beneficial owners to persons that prove their legitimate interest. Member states may impose restrictions on access to all or some of the information on actual ownership in exceptional cases where such disclosure might put the beneficial owner at risk of fraud, blackmail, abduction, violence, or

intimidation. Public registers of beneficial owners will certainly help identify suspicious financial activities and prevent terrorist financing and other criminal activities linked to money laundering.

For example, article 17 of the GDPR gives people the right of deletion, which is also known as the right to be forgotten. However, this is not an absolute right that can always be exercised. Generally speaking, where it is necessary to continue processing such personal data (e.g. because of a legal obligation), the company is permitted to do so. However, each claim should be considered on its merits, and if the company decides not to delete personal data where deletion is requested by the data subject, the company should be able to give valid reasons for failure to do so.

It is important to note that the GDPR has reduced the role of the government to checking evidence in the event of a person's consent. This function has been delegated to a special-purpose government agency: each member state's information controller. If an entity or person gathering information on EU nationals is unable to present documentary evidence of prior consent, the information controller has the power to prohibit such activity.

However, where any personal data processing done by companies is covered by the GDPR, it should give member states the power to have particular rights and obligations restricted by law in special cases where such restriction is a necessary and reasonable measure in a democratic society to guarantee the protection of particular key interests, including public safety and preventing, investigating and detecting or prosecuting crimes, or enforcing criminal penalties, including safeguards against threats to public safety and their prevention. This is important, for example, for AML purposes.

Another important principle is transparency, which requires a company to provide complete information to persons whose rights are affected by personal data processing. Best practice can be a document signed by the customer to confirm his awareness that the company is using his personal data and that he consents to such use by signing the document.

Large companies should first put a system in place to govern personal data based on a compliance system. This should include the following steps:

- Draw up a policy on the protection and safety of personal data;
- Assess all the risks and consequences of personal data processing activities;
- Provide staff with regular training courses to develop their personal data protection skills;
- Retain a wide range of documents describing all the data processing activities and all possible personal data protection breaches.

The two pieces of legislation should eventually be able to work together, and so we now need to help the GDPR take its legitimate place by implementing it and identifying any weaknesses.

[1] 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