VOICU FILIPESCU
Attorneys at Law
News in Laws – Legal Monthly Newsletter
May 2019

cover article

by Marta Popa, Senior Partner Voicu & Filipescu

GDPR – One Year Down, Forever to Go

At least in theory, the General Data Privacy Directive (GDPR or the "Regulation") was the Year2k in data privacy, not only in Europe, but worldwide. Certainly, organizations around the world scrambled to comply with it, fearing very onerous consequences for noncompliance. But the GDPR often vaguely written and does not provide single or sufficiently clear solutions, so compliance in many cases has been a guessing game. So, a year later, where are we? Have things cleared up enough so that we now have some clarity?

2018 – GDPR takes effect and national law is adapted

Shortly after the entry into effect of the GDPR, national legislation received new provisions for adapting the GDPR to the local context. Thus, Law no. 190/2018 has brought on a few special requirements for processing of certain categories of personal data as well as a few derogations from processing personal data in certain situations (e.g. for journalistic purposes). The Romanian Data Protection Authority has proven to be active in issuing secondary legislation regulating situations when the data protection impact assessments are mandatory or the procedure for receiving and solving complaints or performing investiations.

GDPR breaches found and the first related penalties

There appeared the first penalties issued by data protection authorities across the EU for GDPR breaches. Some examples include:

- Facebook was fined £500,000 for collecting personal data about the Facebook friends of users, without those friends being informed that their data was being collected, and without them being asked for consent.
- The Polish Data Protection Authority (UODO) applied the first fine on the basis of GDPR to a data broker for non-compliance with the information obligation under Art. 14 paragraph (1) and (2) of the Regulation. The fine applied amounts to EUR 220,000.
- Uber were fined £385,000 for inadequate security arrangements that led to cyber attackers being able to download a large amount of personal data about drivers and customers.

Some penalties are within the financial penalty limits permitted by the data protection legislation prior to the GDPR and you might think that not much has changed in this regard. However, CNIL (the French data protection regulator) **imposed a fine of 50 million euros against Google, a significantly higher award than that**

provided under the previous legislation. CNIL said Google's processings in relation to its advert personalization lacked transparency, contained inadequate information and lacked valid consent.

What next?

What is on the horizon with regards to GDPR? Well, we must expect that there will be further legislation in the data protection and electronic communications area including the E-Privacy Regulation. We will see increased enforcement and impact in day-to-day activities, including application of significant fines and other penalties. We may also expect that Brexit will impact data protection obligations for some companies. Other future concerns include those regarding Artificial Intelligence (AI) and liability of robots.

Activity in the name of GDPR compliance is thus expected to increase rather than decrease in the second year. True privacy protection and ultimate compliance with GDPR and other privacy regulations is going to require more effort and more investments than anyone likely foresaw.

What can you do if you haven't complied with the GDPR during 2018? Or if you are not sure you have implemented GDPR correctly?

Here is a (non-exhaustive) GDPR compliance list that any company should check:

Action	Concrete Measures
Awareness at Company level. Establishing a framework of corporate governance and responsibility	Inform your employees about GDPR implementation and give them training on the core principles and essential elements of this new regulation. Compliance with GDPR requires actual support at board level but is a team effort. Recommend to the board the GDPR risks and opportunities. Name a GDPR project manager. Incorporate the risk of data protection in corporate risk management and internal control.
Making a data inventory and mapping the data flow	Perform an internal investigation to map operational activities that involve processing of personal data, identify such data, what are the data collection channels, and whether you transfer them outside of the company. Prepare the processing activities registry. Assess the legal basis of your company's data processing.
Performing a detailed gap analysis	Perform an audit of the current state of compliance with GDPR requirements as well as the list of steps to take for

	compliance. Pay particular attention to the impact of GDPR on employment relations.
Creating operational policies, procedures and processes	Prepare the supporting documents for these policies in order to ensure implementation of set rules.
Ensuring personal data security through procedural and technical measures	Implement the "adequate technical and organizational measures" under the IT Security Policy that you establish. Keep in mind the principles of Privacy by design and Privacy by default.
GDPR Compliance of electronic communications	Check and ensure GDPR compliance of electronic communications used at company level (e.g. email, internet, CCTV, GPS applications).
GDPR Compliance of the company's website	The website is your company's business card but also an important way to interact with existing customers, potential customers, or simple visitors. Make sure that the interaction is GDPR-compliant.
Continuous GDPR monitoring and compliance	Set up corporate rules to permanently monitor GDPR compliance, which should include at least periodic internal audits, updating of personal data protection processes, internal processing registers, periodic employee training, testing of IT security systems. For companies which made internal efforts to comply with the GDPR, use of an external GDPR consultant is most recommendable in order to audit the compliance level and remedy any deficiencies.

What can the Voicu & Filipescu data protection team do for its clients:

- Data protection audits and trainings
- GDPR implementation and continuous compliance
- Assuming the DPO position
- Assuming the position of UE representative of companies based outside the Union which process EU citizens' personal data.

Do not hesitate to contact us for any of these services. GDPR is not here today and gone tomorrow!