MPR PARTNERS
MARAVELA, POPESCU & ROMAN

KEY TAKEAWAYS FROM THE PRACTICE OF THE ROMANIAN DATA PROTECTION AUTHORITY

One of the major changes pursued in the data protection field has been the harmonisation of the legislative framework across the European Union (the "**EU**"), target achieved by the enactment of the Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"). Keeping in mind its legal nature – that of a regulation directly applicable in EU member states, and the fact that GDPR provides increased investigative and corrective powers for supervisory authorities, it is crucial to take an in depth look to the decisions issued by the data protection authorities.

The article herein addresses the decisions issued by the Romanian Data Protection Authority (the "**DPA**") since GDPR became applicable.

1. Statistics

In a press release of the DPA[1], referring to 2019, it is stated that 6,193 complaints have been received and 912 investigations have been carried, out of which 385 investigations were triggered by notification of personal data breaches.

Seeing the numbers above, one may think that the DPA's intense activity would have also led to a tremendous number of fines. Actually, the DPA's investigations led to 32 fines, in a total amount of RON 2.365.291,75 (roughly EUR 490,000), to 128 corrective measures and to 134 reprimands.

It is clear that in the last 2 years, the DPA had quite a lenient approach, preferring to issue reprimands and to apply corrective measures, but in the future, we might see a stricter

[1] Press release available at https://www.dataprotection.ro/?page=Comunicat_de_presa_statistica_1_an_GDPR&lang=ro.

approach towards enforcing GDPR's provisions.

2. Type of infringements sanctioned by the DPA

For our analysis, we decided to group the infringements based on their object, considering the GDPR's provisions.

2.1. Security of processing

A significant number of fines and reprimands were issued by the DPA for the infringement of GDPR - article 32 that obliges the controllers and processors to implement technical and organisational measures appropriate to the risk of processing.

Human factor plays an important role in terms of ensuring the security of processing. Analysing the list of fines imposed by the DPA, we have noticed that in a couple of cases, the infringements have been caused by the employees of the data controllers/processors, as follows:

(i) in one case, the employee has accessed the reservation application of the company and photographed the list containing the personal data of 22 passengers – customers of the company. The list has been published online, which led to an unauthorized disclosure of personal data;

(ii) in another case, a company has been sanctioned because it did not take technical and organizational measures in order to ensure that the employees process personal data only at the company's request. In this respect, a list containing the names of 46 persons having breakfast to a hotel has been photographed by a person outside the company and disclosed online. It is not clear whether the employee allowed inadvertently or on purpose the person to take a photo of the list;

(iii) other two companies were sanctioned because some employees of one company worked together with some employees of the other to access information outside the ordinary course of business. In short, the employees of the first company interrogated the databases used internally in order to determine if data subjects – customers of the latter – could be eligible for receiving a loan. Besides breaching the internal procedures, these employees exchanged personal data of more than one thousand data subjects via WhatsApp.

The infringements mentioned above led to the highest fines applied by the DPA (a total of roughly EUR 205,000).

What can be learned from these companies' experience? That they need a strong data protection culture embedded into the organizations. It is vital for the companies to tailor the internal trainings considering their business and the roles and responsibility of each

employee. Data protection can be a game changer and a differentiator, and all employees should be made part of this culture of respect towards the same. This can be achieved if the companies will try to provide practical insights, in which the employees are explained the risks posed for the company if they act against or fail to observe the rules set out in the internal policies, and to make the employees understand that they need to treat customers' personal data in the same manner they expect other companies to treat their own personal data.

In addition, the obligation imposed by GDPR - article 32 must be construed by the data controllers/processors as a duty to observe the particularities of the processing. The controllers and the processors must first identify the specific risks that may be triggered by the processing. The appropriate measures shall be taken based on this analysis. Also, a proportionality test may be done in order to assess which of the identified risks are likely to materialize and whether the measures in place can achieve the level of protection needed.

Based on the rationale behind the applied fines, the key here is striking a balance of appropriateness. Common measures taken by the controller/processor, without an analysis of the specificity of the processing, are not enough to prove compliance and to avoid a fine imposed by the DPA.

2.2. Privacy by design and by default

Three fines have been issued for non-compliance with the provisions of GDPR - article 25 that imposes on controllers a duty to implement appropriate technical and organisational measures at the time of the determination of the means for processing and at the time of the processing itself.

In the first fine issued by the DPA, a bank infringed the privacy by design and by default provisions as the system would automatically disclose to the payment recipient the payer's personal identification number and address. Besides the breach of the data minimization principle, the impossibility to address this technical issue has cost the company EUR 130,000. In accordance with GDPR- recital 78, privacy by design requires that when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, the producers of such should be encouraged to take into account the right to data protection and to set strategies that incorporate privacy protection throughout the life cycle of an object (whether it is a system, a hardware or software product, a service or a process).

2.3. Lawfulness of processing

Failing to observe the lawfulness of processing was yet another common infringement, sanctioned by the DPA.

In many cases, the companies either were not able to prove how they obtained the consent for processing the data subjects' personal data nor did the same use an appropriate legal basis for the processing.

In one particular situation, it will be interesting to analyse the interplay between GDPR and the Law no. 506/2004 with regard to the processing of personal in the electronic communications field ("**Law 506/2004**")[2] and how, depending on the context and the elements of the case, the sanction can be applied either based on GDPR or on Law 506/2004. However, given the fact that there were a lot of discussions around this case, and that there is a pending case before the court we will analyse it with another occasion.

2.4. Right of the data subjects

When it comes to the rights of the data subjects, the following situations occurred on the DPA's radar:

(i) controllers did not reply or could not prove they have replied to the data subject's request;

(ii) controllers did not reply to the data subject's request within the 1-month time frame;

(iii) controllers did not implement, in an appropriate manner, the data subject's objection to the processing of personal data.

The most common situation is related to the improper implementation of the right to object. Numerous complaints were submitted to the DPA indicating that the data subject continued to receive commercial communications even though the data subject objected to receiving such. In some cases, the issue at hand was the delay between the implementation of the request and the propagation of the updates in all of the databases pertaining to the controller and in some cases in the databases of the processors responsible with the transmission of commercial communication. In practice, these databases are not updated in real time, but according to an update cycle (e.g. once every week). What should a company do in such cases? It is important to be completely transparent about the process and to inform the data subjects that a number of days are needed for implementing his or her option and that in this period it is possible for he or she to continue to receive other commercial communications.

Also, it is advisable to periodically revise the systems containing the data subjects' preferences in order to be able to identify possible errors in implementing the same. This recommendation follows a case where the data subject continued to receive commercial

[2] Law 506/2004 transposes into the national legislation Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

communications several months after the data controller confirmed the implementation of his or her request to not receive such commercial communications.

2.5. Other types of infringements

Four fines and several reprimands have been issued for the refusal to cooperate with the DPA during the investigations, by failing to provide the requested documents and information.

Another two fines have been issued for excessive processing of the employees' personal data – image and fingerprints – in the workplace. Moreover, the DPA sanctioned the fact that no legitimate interest assessment was performed in order to justify the chosen legal basis.

The non-observance of the accuracy principle, based on which the data needs to be accurate and kept up to date, by sending, for example, invoices to a wrong address, will also trigger fines from the DPA.

It is interesting to mention that in one case the DPA decided to issue only a reprimand for an unauthorised disclosure of data consisting in sending to several recipients a series of e-mails intended to a client of the company, while in another similar case, where a person received the invoices of another client, the DPA decided to issue a fine. One of the reasons for the difference in treatment might be the fact that in the latter, the company did not act on the complaint of the data subject and this might be an important lesson for the companies.

3. Conclusions

Within these 2 years since GDPR became applicable, the DPA's activity in the enforcement field became more intense, following the trend that emerged across the entire Europe. Some lessons, as mentioned above, may be learnt from the misdeeds of the companies that have been fined or reprimanded until now. It becomes clear that the DPA's level of leniency is gradually dropping while the companies' level of compliance is expected to gradually increase.

The following key takeaways emerge from the decisions issued by the DPA until now:

(i) the human factor plays a considerable role in the case of a personal data breach;

(ii) when implementing measures to mitigate risks, the nature, scope and purpose of the processing must be considered;

(iii) it is crucial that to think privacy from the beginning of any project and to implement the necessary safeguards in order to preserve it;

(iv) one must keep in mind that not only GDPR regulates the processing of personal data;

(v) the safest approach when it comes to data subject requests is for sure not ignoring them. Also, it would be preferable not to wait for several requests from the data subject in order to act on the request;

(vi) it is important to cooperate with the DPA during the investigations and to respond in due time to its request of information and documents.

As a general remark, we consider that it is needed for the companies to create more communication bridges with the DPA, in order to better understand and implement the legal framework.

Even more, the companies should keep in mind that drafting policies and procedures is not only for the sake of doing it, but to pursue the ultimate goal of the GDPR – that of enhancing the protection of people's personal data. Thus, a thorough assessment of the data processing activities and a practical approach with respect to the measures that need to be taken will better help safeguard the personal data and would be more than welcomed in today's context.

******

Cristina Crețu

Senior Privacy & Technology Consultant

cristina.cretu@mprpartners.com

Mădălina Moldovan

Associate

madalina.moldovan@mprpartners.com