IP, IT & Data Protection

GDPR Implementation and Enforcement after one year

May 2019

A Pan-European comparative analysis including infringements and sanctions

France

"In France, a 50 million euros fine has been imposed by the *Commission Nationale de l'Informatique et des Libertés* (CNIL) on Google LLC by a decision n° SAN 2019-001 of January 2019. This decision is the first decision issued in view of the enforcement of GDPR.

The CNIL found that Google is in breach of GDPR obligations relating to transparency and information, the information given being "*diluted in several documents*" preventing the user from being properly aware of their extent. CNIL also found that Google does not comply with the obligation to have legal basis for data processing with respect to advert personalization and does not have valid consent.

Google has brought appeal against this decision before the *Conseil d'Etat* claiming, in particular, that CNIL does not have jurisdiction over Google LLC. Google LLC considers that its head office in Ireland constitutes its principal establishment in Europe and that only the Irish Data protection Commission had jurisdiction. This matter is still pending."

Spain

In Spain, since the GDPR came into force there have been some developments. A new privacy law (LOPDGDD) developing some aspects from GDPR was passed in December 2018.

During 2018, the number of data subject's complaints filed to the DPA (*Agencia Española de Protección de Datos*) raised by 33% in relation to the previous year.

The involvement of the DPA regarding raising awareness and GDPR implementation orientation and support has been enormous and several support tools and guidelines have been issued.

There have not been specific sanctions awarded since GDPR became enforceable; rather, the DPA has focused in analyzing infringements and sending warnings to the respective countries. This is the case of two different decisions, similar but not identical, concerning schools and personal data and photos from students, where the DPA took into account the efforts deployed by both of the schools in data protection measures taken both prior and after the data privacy event occurred.

Germany

Since the EU General Data protection Regulation (GDPR) came into force in May 2018, German data protection authorities have issued 75 GDPR-related fines. The total amount of fines shall amount to EUR 449.000.

The highest fine in a single case in Germany is reported to have been EUR 80.000 and was imposed because of leaked health data due to inadequate internal control mechanisms. In another case, the data protection officer in Berlin had imposed a fine of EUR 50.000 against a bank that had processed unauthorized data of former customers. A German social network had to pay a fine of EUR 20.000 for storing user data unencrypted on old servers.

However, overall, the fines have been kept within reasonable limits. On the other hand, it can be assumed that some more sanctions will follow in 2019. Some German data protection authorities have already made clear that they made will carry out unannounced inspections and increased the number of employees.

Besides, overall, it can be summarized that awareness of data protection has risen sharply in Germany. The companies have "tidied up" their databases, have gained an overview of their data protection processes and adjusted their processes to meet the GDPR requirements.

However, smaller German companies and associations are complaining about the high level of bureaucracy involved, in particular with regard to information and documentation obligations. Even the Federal Data Protection Commissioner in Germany considers in his annual report to reduce the bureaucratic expenditure for small companies and associations.

Austria

Since the GDPR came into force in Austria there have been noticeable changes, even if these have not turned out to be dramatic yet. Regarding the changes, the number of complaints rose rapidly between 2017 and 2018 (the number at least tripled). On the other hand, the highest penalty of € 4,800 currently imposed in Austria is manageable.

But beware! Despite these currently still manageable penalties, a change in jurisdiction of the Data Protection Authority (DPA) can be seen. The requirements of the DPA towards the controllers have noticeably increased, especially regarding security standards (esp in the health care business) as well as information requirements and formal requirements of consent and video recordings. In practice, hundreds of invalid consents might be commercially more painful than a fine, because the relevant data cannot be used legally anymore, and claims for damages might incur. What current decisions show, one should not rely on the in Austria until-now practiced "consulting instead of punishment" initially promised by politicians. At least now, everyone should be GDPR compliant.

Poland

Since the GDPR came into force, we can see intensified efforts of the Polish Supervisory Authority. Throughout this period, the Authority (PUODO) has provided extensive guidance and announced a plan of inspections for 2019. The plan involves primarily public entities, the financial sector and companies engaged in telemarketing. The Supervisory Authority has declared to pay special attention to video surveillance and personnel recruitment.

By now there have been two administrative fines imposed in Poland. The first one of nearly PLN 1M (ca. EUR 230k) was imposed on a company which used personal data of Polish entrepreneurs in its business activity. The data was collected and presented on the company's website, while the data subjects were not informed thereof in the manner required by Article 14 of the GDPR. The other case involved a regional football association which published names, addresses and personal identity numbers of 585 licensed referees on its website. The fine was PLN 55k (ca. EUR 13k) and was reduced because of good cooperation, compliance with PUODO's instructions and the fact that none of the referees suffered any damage. These were not the only infringements identified by the Authority, but the other breaches were not fined.

The GDPR raised much concerns among Polish entrepreneurs in May 2018. However, it also considerably raised awareness of the personal data protection issues. Moreover, the GDPR positively influenced some Polish SMEs who are now more careful processing the data and make efforts to ensure compliance in this respect.

The GDPR has some side effects in Poland with GDPR-trolling in the lead. People literally spam Polish companies with personal data-related requests, hoping to discover a breach and a cause for claiming damages. So far, to the best of our knowledge, such attempts have proved futile.

Italy

"In Italy we can say that it has been few days from the beginning of the full application of new penalty regime provided by GDPR.

Although the GDPR came into force on 25th May 2018, Italy provided a "soft period", by means of the article 22, paragraph 13, of Legislative Decree 101/2018 – according to which during the first eight months, starting from September 2018, the Italian Data Protection Authority does not impose any GDPR related penalty. This "soft period" passed on May 19th.

During 2018 Italian Data Protection Authority focused on issues related to malicious software, aspect in labour law, cybersecurity, healthcare, electronic invoicing and telemarketing, as underlined by the President of the Authority during the 2018 activity report."

Hungary

Since the entry into effect of the GDPR, the Hungarian data protection authority (NAIH) has imposed administrative fines in the range of HUF 500,000-1,000,000 (ca. EUR 1,500-3,000); on one occasion, it imposed a fine of HUF 11,000,000 (ca. EUR 34,000). The smaller fines were related to the violation of miscellaneous data protection requirements, such as the failure to provide sufficiently transparent information to a customer request (the customer wanted to know how his data stored in back-up copies are processed and for how long), or the failure by the controller to restrict the usage of a telephone number when the new owner of the number indicated that the number no longer belongs to the customer from whom it was originally collected. One important decision stated that, in the context of a car financing loan, the use of a telephone number for the purpose of debt collection, which is a purpose different from what was communicated to the data subject at the time of collection of the data, is a processing about which the controller should have informed the customer, and a processing which shall be justified by a balancing test performed specifically for such purpose – a general reference to the controller's legitimate interests is not sufficient (the balancing test has to be performed in respect of each purpose). The case in which the NAIH imposed a fine of HUF 11,000,000 (ca. EUR 34,000) involved a website data breach affecting 6,000 persons and the leakage of their data about their political opinions, in addition the controller failed to comply with its obligation to notify the breach to the data protection authority."

Greece

The Greek Data Protection Authority has issued a rather small number of decisions under the GDPR. In such decisions the Authority had been rather lenient, as it opted for issuing reprimands to controllers instead of imposing fines.

In the three cases regarding failure to comply with the obligation of notification of personal data breach, the Authority issued a reprimand, taking into account the fact that (a) GDPR had just started been applicable; (b) the controllers reacted immediately and promptly and dealt efficiently with the data breach; (c) the data breach concerned a very limited number of natural persons; (d) the hacking attack reported in one of the cases was unknown and advanced.

In the one case pertaining to non-compliance with the obligations regarding non-solicited advertising communications, the Authority opted for a reprimand on the basis of the fact that it was just one natural person complaining to have received advertising messages through Viber without having provided consent pursuant to the relevant provisions of the GDPR. It is crucial, in the Authority's view, to provide sufficient information to the natural person, and to state clearly the purpose of the processing, i.e. whether it is within the context of the contract, or it is of a promotional nature.

It is, however, to be noted that in cases decided under the previous legislative framework, the Authority seems to have become stricter in the imposition of fines, and in certain cases it has reached the maximum limit of 150,000 Euro.

Furthermore, the authority has announced that it has carried out more than 65 self-initiated remote investigations on the websites of companies in various sectors of the economy, with a view to monitoring compliance with a number of obligations under the GDPR. The authority has issued notices to the controllers, ordering them to bring processing operations into compliance with the provisions of the GDPR within a specified deadline, in some case by taking certain specified measures proposed by the Authority, and to inform it accordingly.

In addition, the Authority has published the list of data processing activities that in its view need to be covered by a DPIA.
Likewise, it is interesting to mention that the DPA has announced that it has received from the 25th of May 2018 until the beginning of this year more than 96,000!!! complaints from data subjects alleging infringement of the provisions of the GDPR. It remains to be seen which part of them is substantiated and as such will result in the adoption of significant enforcement decisions by the Data Protection Authority.

Finally, it should be noted that Greece has not yet adopted legislation to cover the areas that are left to the jurisdiction of the Member States.

Romania

Since the GDPR came into force, there have been some noticeable data privacy developments in Romania. In 2018 the Romanian Parliament has passed Law no. 190 which addresses some of the" open" points in the GDPR. At the same time, Directives 2016/680 and 2016/1148 have been transposed in the national legislation.

In terms of second tier legislation / best practice guides, the involvement of the DPA is rather poor. Some professional associations representing controllers in banking, telecom or publishing sectors have submitted codes of conduct for DPA's approval but, as per our knowledge, none of such codes have yet been approved by the DPA. Instead, the DPA chose to raise awareness at an informal level, by participating to many local conferences and events dedicated to GDPR, organized by both public and private sector.

The DPA's investigations generally focused on solving complaints on alleged data privacy breaches, which increased significantly since GDPR came into force. In 2018, the number of complaints filed after 25 May was 2.5 times higher than the number of complaints filed before the GDPR came into force. Nevertheless, the DPA has also opened *ex officio* a series of sectorial investigations - we are aware of investigations being already opened in banking sector. Not least, the DPA pays particular attention to security breaches - they are already investigating a series of breaches.

We are not however aware of specific sanctions applied by the DPA for GDPR non-compliance. Yet, in line with the general trend at the EU level, it is expected that fines and other sanctions (including corrective measures) for GDPR non-compliance are issued rather sooner than later.

Portugal

One of the first sanctions imposed after GDPR became enforceable was to the Hospital of Barreiro, one of the most populous public hospitals of Lisbon region. The infringement related to the indiscriminate access to clinical data. The sanction was grounded on the following infringements of GDPR: the data minimization principle; because the Hospital allowed indiscriminate access to an excessive data set for professionals who could only access them in cases previously justified; integrity and confidentiality principles, for failing to implement organizational and technical measures aiming to prevent unlawful access to personal data; inability of the Hospital to ensure integrity, confidentiality, availability and permanent resilience of systems and processing services and failure to implement appropriate organizational and technical measures to ensure a level of security appropriate to the risk, in particular a process to test, assess and evaluate regularly the effectiveness of the security measures of data processing. The Portuguese DPA (CNPD) imposed on Hospital of Barreiro a fine in the sum of 400.000 euros.

Andersen Tax & Legal | Service Line IP, IT & Data Protection

Special thanks to the contributors:

> Spain · Belén Arribas · belen.arribas@AndersenTaxLegal.es
> Germany · Dr. Fritjof Börner · fritjof.boerner@AndersenTaxLegal.de
> Portugal · Raquel Brízida Castro · raquel.castro@AndersenTaxLegal.pt
> Romania · Bogdan Halcu · bogdan.halcu@tuca.ro
> Greece · Dr. Themistoklis K. Giannakopoulos · themistoklis.giannakopoulos@AndersenLegal.gr
> Italy · Francesco Inturri · francesco.inturri@andersentaxlegal.it
> Poland · Magdalena Patryas · magdalena.patryas@ksplegal.pl
> Austria · Katharina Raabe-Stuppnig · raabe@lansky.at
> Hungary · Tamás Szabó · tamas.szabo@sz-k-t.hu
> France · Angélique Vibert · angelique.vibert@AndersenTaxLegal.es