IP, IT & Data Protection

GDPR Implementation and Enforcement

November 2019

A Pan-European comparative analysis including infringements and sanctions in the past year and a half

As of May 25, 2018, Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 272016, the General Data Protection Regulation (hereinafter "GDPR") entered into force.

The GDPR offers a new framework for data protection with increased obligations for organizations, and its reach is far and wide. The GDPR is applicable to any organization — no matter where it resides — that intentionally offers goods or services to the European Union or that monitors the behavior of individuals within the EU.

While GPDR has helped raise awareness of the public regarding privacy rights – notably, over 300.000 cases reached the national data protection authorities, with 150.000 individual complaints; over 400.000 DPOs were appointed and registered; 90.000 data breach notifications were carried out and sanctions awarded across the EU amount to millions of euros- a number of companies, lobbies and institutions have expressed criticism and described the challenges associated in their opinion with the GDPR, including the various ways in which the law has impacted businesses, digital innovation, the labor market, and consumers.

One of the challenges described relates to its alleged lack of consistency in its implementation across member states. We have therefore endeavored this "Pan-European comparative analysis including infringements and sanctions", first published in May 2019 (read more here) and now updated.

The countries analyzed are the following:

- Spain
- Germany
- Austria
- Poland
- Italy
- Hungary
- Greece
- Rumania
- Portugal

Spain

In Spain, since the GDPR came into force there have been some developments. A new Spanish 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. Similar growth is expected until the end of this 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.

While in the first months after the GPDR became enforceable the Spanish DPA has primarily focused in analyzing infringements and sending warnings to numerous companies, after a while specific sanctions started to be published, with a total now of 15 sanctions published at the time of closing this article.

The higher fine so far is the one of EUR 250,000 against "La Liga" on the merits of an application that uses the geolocation and the microphone of the mobile phone of millions of service users in order to combat piracy in public establishment that broadcast soccer games without a license. According to the DPA, this application was not compliant with transparency requirements on such processing and did not allow users to revoke consent.

Regarding warnings issued by AEPD, two must been highlighted; 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.

Other important published sanctions include companies from different sectors.

- Two telecom companies were fined EUR 60.000 and 36.000, respectively, for lack of legal basis in their processing, as they had used personal data for the conclusion of a telephone contract without consent, in one case, and the telecom company has continued to process personal data even when the data subject requested that the processing be discontinued, in the other case.

- A cosmetics company was awarded with EUR 60.000 sanction for unlawfully processing a subjects data without adequately verifying his/her identity, which led to his/her data erroneously entered in a register of claims, consequently preventing him/her from operating with his/her bank.

- An airline was sanctioned with EUR 30.000 for insufficient legal basis to process data since users did not have the ability to refuse their cookies, as it was not possible to browse their webpage without accepting their cookies.

- A debt collection company was sanctioned with a EUR 60.000 fine for insufficient legal basis for data processing in a case where a claimant who allegedly did not pay back a microcredit started receiving claim emails not only to the email addresses provided by him but also to an email address of his workplace which was accessible by any co-worker; such email address was never provided by the claimant.

Other lesser sanctions involve gas companies, online gaming operators, electric and utility operators, but also SMEs and other, ranging from EUR 12.000 to 1.000, on the basis of different law infringements.

Germany

Since the EU General Data protection Regulation (GDPR) came into force in May 2018, German data protection authorities have issued more than 100 GDPR-related fines. The total amount of fines shall amount to about EUR 1.5 million.

The highest fine in a single case in Germany was reported recently, about EUR 14.5 million, and was imposed against a real estate company (Deutsche Wohnen SE). The company had collected and stored a huge number of personal data of their tenants in an archiving system for years, without checking if this was necessary and legally permissible. A first complaint by the data protection authorities in 2017 had been ignored. However, the decision is not final yet, as Deutsche Wohnen might claim against the fine.

Similar to the previous case, a food delivering company took a fine of about EUR 200.000 because they had not deleted the accounts of former customers, in ten cases, even though those data subjects had not been active on the company's delivery service platform for years.

In another case, a data protection officer in Berlin 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.

Overall, most fines have been kept within reasonable limits in Germany. However, it can be assumed that some more sanctions will follow in 2019. Some German data protection authorities have already

made clear that they will carry out unannounced inspections. They are also increasing the number of employees.

It can be summarized that awareness of data protection has risen sharply in Germany. 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, reducing 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 EUR 4,800 currently imposed in Austria is manageable.

But beware! Despite these currently still manageable penalties, a change in the 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 (especially in the healthcare sector) as well as information 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.

In 2019, the proceedings in front of the DPA have increased – and so have the fines. An allergy center was fined EUR 50,000 for non-compliance with information obligations and for not appointing a data protection officer even though they were obliged to do so. Another fine was imposed upon a soccer coach who – for years – filmed female players in the shower. Even though this does not constitute a crime (the criminal charges were dropped), there was a EUR 11,000 fine for violation of privacy.

Other interesting decisions included the clarification of the DPA, that anonymizing is a legitimate way to fulfill a deletion obligation, and that – regarding a site to review doctors – the interests of potential patients for information outweighs the interest of the doctor not being included in this site.

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 five 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.

The third fine of nearly PLN 3M (approx. EUR 660k) was imposed on 10 September and publicized on 19 September. The fine was imposed on a well-known online shopping site selling electronics, which was found to have failed to apply adequate technical and organizational measures to ensure protection and safety of information, which resulted in personal data leak in a hacking attack. The personal data of approx. 2.2 million people were found to have been accessed by unauthorized persons. Subsequently, the data was probably sold on the Darknet. Moreover, the data of 35 thousand customers affected by the leak included financial details, because the sale was made on a hire-purchase basis. Furthermore, the personal data affected were used for sending phishing messages containing a demand for payment of an additional fee. This was considered by PUODO a violation of the rights and freedoms of data subjects. The penalised entity informed that it was going to file an appeal.

The fourth fine was imposed on a public body due to continuous infringement of Art. 5 of the GDPR, consisting of the failure to: (i) conclude a data processing agreement with a web hosting service provider, (ii) conduct a risk analysis for some data processing activities, (iii) prepare the data retention policy, (iv) create backups for certain data processing activities. The fine amounts to approx. PLN 40k (ca. EUR 9.3k), which is relatively low, but it bears emphasizing that the Polish Personal Data Protection Act provides for a limit on fines for personal data breach that can be imposed on a public entity, which is PLN 100 thousand (approximately EUR 23k).

The fifth fine of PLN 200k (approx. EUR 47k) was imposed on a provider of e-mail, SMS or phone marketing campaigns. The PUODO considered the process of withdrawing consent for marketing purposes not sufficiently easy and discovered that the provider continued to process personal data even though the data subjects requested erasure of their personal data or submitted an objection to their processing.

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.

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 labor law, cybersecurity, healthcare, electronic invoicing and telemarketing, as underlined by the President of the Authority during the 2018 activity report.

In 2019 the Italian Data Protection Authority issued several judgments involving the so-called "right to be forgotten”. In particular, the Data Protection Authority stated “the right to be forgotten” of a person who had obtained criminal rehabilitation, in consideration both of the time that had passed since the facts took place and of the disproportionate negative impact - on the data subject’s rights - of the further processing of those personal data – that had not been updated – through the persistence, on the Internet, of the disputed URLs.

Moreover, the Data Protection Authority has issued many decisions regarding data breach. In one case, pursuant to Article 58(2) point (e) of the GDPR, the Authority ordered a company (one of the leading national email provider) to communicate again the data breach to the data subjects involved in a fraudulent access to the Wi-Fi network that had caused the violation of approximately 1.5 million e-mail credentials. According to the Italian Authority, in fact, the communication already sent to the data subjects were not compliant with the provisions of Article 34(2) of the GDPR, also considering that the

said communications were sent to the same email accounts whose authentication credentials had been breached.

Furthermore, with regard to data breach, on July 30, 2019 the Data Protection Authority provided a notification form that controllers may use to notify to the Data Protection Authority the details of the data breaches occurred.

Hungary

Since the entry into effect of the GDPR, the Hungarian data protection authority (NAIH) has imposed administrative fines in the range of ca. HUF 100,000-11,000,000 (ca. EUR 300-34,000); on one occasion, it imposed a fine of HUF 30,000,0000 (ca. EUR 91,000).

Notably, the NAIH has imposed significant fines not only on market participants, but on public authorities, too – HUF 5,000,000 (ca. EUR 15,000) on the police for its failure to notify the loss of a pen drive containing the personal data of 1,733 employees; and HUF 3,000,000 (ca. EUR 9,000) on a court of law for keeping record of certain individual judges' affiliations. The most severe administrative fine to date has been imposed on the organizer of summer festival events, in the amount of HUF 30,000,000 (ca. EUR 91,000). In this case, the NAIH has found that the organizer stored more personal data than necessary for the stated purposes (the visitors' IDs had been scanned and the data contained in the IDs had been linked to the tickets as a condition of entering the festival area for the purpose of crime prevention, preventing and fighting terrorist attacks, and preventing the touting of tickets, but the NAIH found that the processing activities had little practical benefit in achieving these purposes). The fine amounted to ca. 2.4% of the company's annual income.

As a general tendency, the NAIH seems to apply the GDPR rules on the legal basis of processing activities rather narrowly and restrictively. Another important takeaway on the basis of recent decisions is that whenever the controller relies on the legitimate interest basis, there must be a well-documented and strongly reasoned balancing test in place, otherwise the NAIH may find the processing to be without proper legal basis.

Greece

In the first months, 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 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 EUR 150,000.

However, by two recent decisions the Greek Data Protection Authority imposed fines amounting to EUR 400,000 in total upon an e-communications service provider. The fines were imposed in the first case, for failure of the data controller to comply with the principle of accuracy and data protection by design when keeping personal data of subscribers. In the second case, failure to satisfy the right of the data subjects to object, and to safeguard the principle of data protection by design when keeping personal data of subscribers caused the imposition of the fine.

These two fines are quite significant in the post GDPR era.

In the first case, the updates of the opt-out registry of the subscribers who had previously exercised their right not to be included amongst the recipients of calls for promotional purposes were not concluded as required, following similar updates in the general customer database. The discrepancies between the files emerged due to technical errors in their interconnection, resulting thus into the receipt of calls with such content by data subjects who had explicitly opted-out to this respect.

In the second case, the recipients of advertising messages were not able to unsubscribe themselves, while exercising their right to object to such processing, using the relevant link available to the advertising messages, due to a technical operational error. Therefore, as emphasized in the Greek DPA's decision not only the right was not satisfied, but also an appropriate organizational measure that could detect this infringement was not in place.

While the Greek DPA assessed the amount of the fines imposed, various circumstances were also considered both as aggravating and mitigating factors respectively. For instance, the significant number

of data subjects affected, the duration of the failure to comply, the main business activity of the data controller, the liability of the latter in a previous data breach incident, along with the former sanction of the "warning" by the Greek DPA with respect to the inclusion of data subjects to the opt-out registry were identified as aggravating factors. However, the lack of intent, the corrective measures taken and the cooperation with the Authority were also considered as mitigating factors.

The principle of data protection by design & by default is established through these decisions as one of a great importance. This principle does not constitute a theoretical prerequisite of compliance, but rather a practical necessity. The decisions echo for the increasing need of internal audits in order to identify similar security gaps and to safeguard that both at the level of determining means of processing, as well as at the time of the processing itself, appropriate technical and organizational measures guaranteeing compliance are in place. Internal audits and implementation of additional technical and organizational measures are the real challenge of the next day. If the entities falling into the scope of the GDPR fail to address it, it is highly possible that they will have to face the relevant sanctions by the competent authorities.

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 several 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. Also, Directives 2016/680 and 2016/1148 have been transposed in the national legislation.

As for the second-tier legislation / best practice guides, the involvement of the DPA has been 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.

Within the first GDPR year, there have been filed 5260 complaints (the number of complaints has almost doubled as opposed to the year before GDPR) and 400 data breach notifications. Interestingly, during the first GDPR year the DPA has opened 496 investigations pursuant to complaints, while approximately same number of investigations (namely 485 investigations) have been opened ex officio.

In terms of fines applied, the highest fine (the 2nd highest fine at that time in Central Europe) was imposed in the banking sector, for a bank's failure to put in place appropriate technical and organizational measures to ensure compliance with the data minimization principle and the principle of data protection by design/ by default. The infringement led to documents comprising the details of transactions, which were made available online to payment beneficiaries, revealing the IDs (personal identification number included) and addresses of over 300,000 data subjects (payers to the accounts opened with that bank).

In another case, a hotel has been fined with EUR 15,000 for failure to implement adequate technical and organizational measures (particularly to ensure that its staff takes appropriate measures to preserve confidentiality of data). This led to the unauthorized access and on-line publication of data (names and meal preferences) concerning 46 customers.

A EUR 3,000 fine has been imposed to a website that, due to improper security measures after a platform migration, allowed public access via two links to a list of files comprising details of several business contacts, which included name, surname, postal address, email, phone, workplace and transaction details.

Also, an organization has been fined with EUR 2,500 for (i) not being able to prove that its employees were adequately informed about the use of a CCTV surveillance system, and (ii) revealing unlawfully on the company's notice board of the name and the personal identification number of certain employees.

Ro DPA (ANSPDCP) has fined Raiffeisen Bank (RB) by EUR 150,000 and a credit broker (Vreau Credit S.R.L.) by EUR 20,000.

RB has been fined for failure to take adequate technical and organizational measures for preventing the unauthorized access and disclosure of personal data. Precisely, two RB's employees have interrogated the credit bureau (a credit risk evidence system) with regard to 1177 clients of the credit broker. The IDs of the clients were being sent by the credit broker to the RB employees via WhatsApp. Furthermore, same RB employees also interrogated the date base of the National Finance Authority (ANAF) for 124 prospects of the credit broker. The employees sent the output of the interrogations to the credit broker, acting thus outside of their job duties. RB has notified the personal data breach to ANSPDCP. Further to such, RB has been fined for not ensuring that the respective RB employees process the data only based on the instructions of RB and in accordance with their job duties.

The credit broker has been fined as well by EUR 20,000 for unlawful disclosure of personal data (IDs) of its clients and failure to notify the personal data breach to ANSPDCP.

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 EUR 400.000.

In addition to the case of Hospital do Barreiro, the Portuguese DPA (CNPD) issued, this year, three other fines on private entities. However, CNPD decided to not disclose the identities of the companies. The highest one was in the sum of EUR 20,000 and involved the violation of the data subject's right of access to his/her data. In the others two cases, CNPD issued fines of 2.000 euros, grounded on violations of article 13/1 and 2, GDPR (Information to be provided where personal data are collected from the data subject), related to use of video surveillance.

On the other hand, this year, our Parliament was invested in a "frenzy behavioural legislative production" on data protection, that, in my opinion, created a regulatory and institutional tangle. Last June, the Parliament approved four new laws on data protection: i) the new law implementing GDPR and the new law developing GDPR only for judicial system, with another DPA. Also, Directives

2016/680 and 2016/1148 have been transposed in the national legislation, one of them with another DPA.

However, the law implementing GDPR only for judicial system was vetoed by the President of the Republic. The law assigns judicial magistrates and the MP of responsibility for the processing of data in the context of processes of its competence and created a new DPA, whose (ministerial) composition is contested and is likely to violate the principle of separation of powers.

Also, through a juridical interesting deliberation, CNPD decided not to apply fifteen articles of the law that implements GDPR, only with a month of life. CNPD justifies that those articles are not compliant with GDPR.

In the last months, CNPD has published two relevant deliberations. First of all, the list of data processing activities that need to be covered by a DIPA. On the other hand, Portuguese DPA also released an Interpretative deliberation on the possibility of public authorities being exempted from fines, provided by the new law, during next three years. Since several public entities have requested this exemption, CNPD decided that can only decide it, in casu.

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
> Poland · Magdalena Patryas · magdalena.patryas@andersentaxlegal.pl
> Italy · Francesco Inturri · francesco.inturri@andersentaxlegal.it
> Hungary · Tamás Szabó · tamas.szabo@sz-k-t.hu
> Hungary · Tamás Kárpáthegyi · tamas.karpathegyi@sz-k-t.hu
> Greece · Dr. Themistoklis K. Giannakopoulos · themistoklis.giannakopoulos@AndersenLegal.gr
> Romania · Bogdan Halcu · bogdan.halcu@tuca.ro
> Austria · Katharina Raabe-Stuppnig · raabe@lansky.at
> Portugal · Raquel Brízida Castro · raquel.castro@AndersenTaxLegal.pt