SROUJI AVOCATS
AVOCATS A LA COUR

www.sroujiavocats.com

Overview of recent data protection fines in the European Union

June 2021

Executive Summary

Despite the economic turmoil created by the global pandemic, the year 2020 and early 2021 were marked by the continuing trend of EU Data Protection Authorities (DPAs) to enforce the General Data Protection Regulation ("GDPR," Regulation 2016/679 of 27 April 2016). This has led to an increase in the number of fines issued as well as an increase in their amount.

The past six months have been especially noteworthy due to a number of record breaking fines. Several DPAs stand out for their aggressive posturing. Firstly, the French DPA, the CNIL (*Commission Nationale de l'Informatique et des Libertés*), imposed on Google, in December 2020, one of the highest fines ever levied by a EU DPA (combined fine of €100 million). Secondly, the Spanish DPA, the AEPD (*Agencia Española de Protección de Datos*), which has historically been very aggressive well before the GDPR came into effect, continues to break its own records as it has issued several significant fines in the past few months.

DPAs have yet to make full use of their full statutory power to levy penalties allowed by the GDPR, which in theory allows for fines of up to 4 percent of a company's annual global revenues. As of now, a small number of fines approach barely 1 percent of the sanctioned company's global revenues.

This tendency of increased amounts is coupled with an increase in the number of fines issued. Between January 2020 and January 2021, the number of fines increased by 40%, and more than 30 fines were issued just in May 2021. This is in part explained by the provisions of the GDPR, which essentially allow for smaller fines to be issued for relatively minor offences.

No economic sector is really spared from this increased enforcement. In the last few months, fines have been imposed on companies in the relatively benign transportation and public sectors – even sports clubs have been sanctioned. There are, however, some obvious business sectors that attract regulatory scrutiny. A majority of the significant fines issued in the last six to seven months were imposed on financial institutions, telecoms operators, technology companies like Google and Amazon, social networks, some dating applications, and more generally speaking, companies whose main activity is based on the internet. The health sector also is subject to special scrutiny.

In the last few months, a significant number of fines were issued as a result of a company's failure to ensure data security and prevent data breaches. The processing and/or transfer of personal data without having obtained valid consent or otherwise not based on a legally valid basis is another hot area. A company is also likely to face regulatory action for aggressive or non-consented marketing practices – a situation that existed well before the GDPR came into effect.

Finally, the growing tendency of DPAs to cooperate to ensure that enforcement action is effective, dissuasive and proportionate, and to work together to manage transnational violations, is increasingly evident. Such was the case with the fines issued in the British Airways and Marriott

International decisions, levied by the UK DPA, the ICO (*Information Commissioner's Office*). These fines were effectively the result of DPA's coordinating via the one-stop-shop mechanism (which allows a DPA in one member state to act on behalf of the entirety of concerned DPAs).

Overview of data protection fines in the European Union

Belgium

- *Unnamed financial institution* - 26 April 2021

The Belgium DPA imposed a €100,000 fine on a financial institution for failure to provide an adequate level of data security.

The case started with a complaint from a former spouse of one of the company's employees. During the process of liquidation of their joint estate, the ex-husband had repeatedly used his access to the Central Individual Credit Register of the National Bank of Belgium to research the personal/financial data of his former spouse. As the DPA noted, the violations occurred due to the fact that the company (the controller of the data), had not taken adequate organizational measures to protect personal data from unauthorized processing.

This is the second highest fine to date in Belgium and highlights the importance of investing in cyber security.

Czech Republic

- *Eleven unnamed companies*, 5 January 2021

The Czech DPA, the Office for Personal Data Protection (the Office) imposed a fine of 3,1 million Czech koruna (approximately €119,000), on eleven companies for sending unsolicited commercial communications.

The companies had processed thousands of pieces of personal data, with no legal basis, to send various goods and services offers. However, the DPA found that the companies had no legal basis for such processing. The DPA also noted that the companies did not provide the data subjects with information about the commercial use of their data when they first contacted them.

This is not the highest fine ever issued by the Czech DPA. Last year, the Office imposed a fine of 6 million koruna for email spamming. However, this decision was pronounced under the Czech Act 480/2004 on Certain Services of Information Society, as known as the Anti-Spam Act. The fine issued against the eleven companies is thus the highest fine ever handed out by Czech Republic under the GDPR. The decision indicates the trend of the Czech Republic to follow the general tendency and provide for a stronger enforcement of the GDPR.

France

- Google & Amazon - 7 December 2020

The French DPA imposed a €100 million combined fine on Google, and a €35 million fine on Amazon, for unlawful cookie usage. The sanction was not based on a provision of the GDPR, but on a French provision (article 82 of the *Loi Informatique et Libertés*) transposing the corresponding provisions of the European E-Privacy Directive (2002/58/EC).

Controls operated by the CNIL revealed that Google and Amazon were depositing cookies without having obtained the prior consent of users. Cookies were simply automatically deposited on the device whenever one of the websites was used. Furthermore, the CNIL considered that the level of information available on both websites did not allow for a freely given, specific, informed and unambiguous consent.

As stated earlier, this is the largest fine ever imposed by a DPA, and shows the will of Data Protection Authorities to strongly enforce data protection laws, especially when a large technology company is involved.

- *Unknown company* - 27 January 2021

The CNIL issued a €150,000 fine to a controller, and a €75,000 fine to its processor, for breaching their obligation to ensure the security of the data they were processing. The negligence of the data security led to a cyber-attack on the controller's website.

This decision is a reminder that both the controller and the processor play an important role in the protection of data privacy, and thus, are both likely to be held liable and sanctioned in the event of a data breach.

Germany

- Notebooksbilliger.de - 8 January 2021

The German data regulator of Lower Saxony imposed a fine of €10,4 million to the company for monitoring employees through constant video surveillance for at least two years, without a legal basis. Some of the areas recorded included workspace, sales floors, warehouses, and staff rooms. The company claimed that the video cameras were installed to prevent and investigate criminal offences. The German regulator responded that general suspicion does not legitimize the use of such a surveillance system, which constitutes in itself a major violation of the employees' rights.

This is the second fine issued by the Hamburg-based data regulator for employee surveillance, after it fined H&M in October 2020. These two cases (Notebooksbilliger.de and H&M) led to the issuing of the two largest fines ever levied by a German regulator.

These decisions can serve as a warning to companies to respect their employees' privacy, as they highlight the seriousness of the infraction in the eyes of DPAs, especially for Germany.

- VfB Stuttgart - 10 March 2021

The German football club VfB Stuttgart was ordered to pay a €300,000 fine for violating the EU's data protection rules. The club was alleged to be selling data to third parties without informing its members of such practices (and thus without collecting proper consent).

Ireland

- Twitter - 15 December 2020

The Irish DPA (Data Protection Commission), issued a fine of €450,000 to Twitter for failure to notify a data breach within 72 hours of becoming aware of the incident and failure to adequately document the breach.

The draft decision in this inquiry has been submitted to and approved by other concerned DPAs. This decision is the first one to go through the GDPR dispute resolution process since the introduction of the GDPR and was the first Draft Decision in a **"**big tech" case on which all EU DPAs were consulted.

- The Irish Credit Bureau - 23 March 2021

The Irish Credit Bureau (ICB), a private financial agency, received a fine of €90,000 from the Irish DPA, for failure to put in place appropriate technical and organizational measures to effectively implement the principle of accuracy.

The ICB implemented a code change in its system which contained a technical error. As a result, the Irish DPA found that the ICB database had inaccurately updated the records of 15,120 closed accounts and provided 1,062 inaccurate account records to financial institutions or data subjects before fixing the issue.

Italy

- Vodafone Italia - 12 November 2020

The Italian DPA, the *Garante*, issued a fine of about €12 million to Vodafone Italia for aggressive telemarketing practices.

The proceeding was initiated by the *Garante* after receiving hundreds of complaints and alerts, against unsolicited phone calls made by Vodafone in order to promote telephone and Internet services. The investigation carried out by the *Garante* revealed major violations of consent requirements, as well as violations of the accountability principle and of the principle of data protection by design. Plus, the most worrying discovery made by the *Garante* was the use of fake telephone numbers or numbers that were not registered with the Italian Register of Communication Operators when placing the marketing calls.

The fine is the third highest issued in Italy under the GDPR, behind two decisions issued earlier in 2020.

- Fastweb - 2 April 2021

This decision is similar to the Vodafone case. The company received a €4.5 million fine for engaging in unsolicited telephone marketing practices without prior collection of the customers' consent. The fine was also imposed to sanction the use of fraudulent telephone numbers that the company had not registered with Italy's Register of Communication Operators.

Netherlands

- Booking.com - 31 March 2021

The travel agency received a fine of €475,000 for failure to report a data breach within 72 hours of becoming aware of the incident.

In December 2018, criminals persuaded hotel staff to reveal the log-in details for their accounts in the Booking.com system, allowing the attackers to gain access to the personal data of more than 4,000 customers. Compromised details included names, addresses, telephone numbers and approximately 300 credit card numbers, and in 97 cases, the credit card security codes were obtained as well. The company only notified the breach 22 days after its discovery.

- Municipality of Enschede - 29 April 2021

The Dutch DPA imposed a fine of €600,000 to the public entity for unlawful Wi-Fi tracking practices.

The DPA found that in 2017 the municipality had used Wi-Fi tracking technology to measure the number of people within the city center. The true intent of the municipality was to simply count people but the employed technology gave them the possibility to track people's cellphones for a longer period of time rather than simply count them. The DPA specified that regardless of the municipality's intent, the use of such technology with no legal basis is, in itself, a serious violation of the GDPR.

This decision underlines the fact that public entities may also be sanctioned under data protection laws.

Norway

- Grindr - 24 January 2021

On 24th January 2021, the Norwegian DPA, the Datatilsynet, notified Grindr LLC of its intent to issue an administrative fine of 1 million Norwegian kroner (approximately 10 million euros).

Grindr LLC is a dating application, which means that the mere use of the application can be linked to the user's sexual orientation – thus, the company processes a special category of data. The primary concern of the *Datatilsynet*, was that Grindr had shared data to a number of third parties for marketing purposes without the users' consent or any other legal basis. The data shared included GPS location, users' profile data, and the fact that the users were on Grindr. The Norwegian DPA considers this as a particularly serious case, which justifies the amount of the fine issued.

To this day, this is the highest fine ever issued by Norway under the GDPR.

- Disqus Inc - 5 May 2021

On 5th May 2021, the *Datatilsynet* declared its intention to issue an administrative fine of €2.5 million (25 million Norwegian kroner), to Disqus Inc (a blog comment service for websites). The company did not comply with the GDPR rules of accountability, lawfulness and transparency.

The *Datatilsynet* was made aware that Disqus conducted unlawful tracking of visitors to Norwegian websites which were using the Disqus plugin. The visitors' data was then disclosed to third party advertising partners.

This is not a final decision as Disqus has been given the opportunity to comment and contest the accusation until 31 May. To this day (June 4th), no contestation has been made public by the Authority.

Poland

- Virgin Mobile Polska - 3 December 2020

Virgin Mobile Polska received a fine of 1.9 million Polish złoty (approximately €460,000), for failure to ensure the security of the data processed by the company, and failure to notify a data breach. The controls carried out by the DPA revealed insufficient security measures, which enabled an unauthorized third party to access a database containing personal data of over 140,000 subscribers to pre-paid services. The disclosed details included name and surname, national identification number, series and number of their ID card, phone number and tax identification number.

This is the second largest fine ever issued by Poland under the GDPR.

- ID Finance Poland - 30 December 2020

The Polish DPA issued a €250,000 fine (1 million Polish złoty) to the financial institution for failure to ensure the security of the data collected and processed.

ID Finance Poland had received a notification about gasps in its IT security but the notification was not treated seriously. A few days later, the institution was subjected to a ransomware attack. This would not have occurred if the company had immediately reacted to the notification that the data on its server was unsecure. Therefore, the Polish DPA found that the company had not implemented appropriate technical and organizational measures to ensure data security.

This is the third largest fine ever issued by Poland under the GDPR.

Romania

- Banca Transilvania - 17 November 2020

The bank received a fine of 487,000 Romanian leu (approximately €100,000), from the Romanian DPA, the ANSPDCP (*National Supervisory Authority For Personal Data Processing*).

According to the ANSPDCP, the bank had failed to provide sufficient technical and organization measures to ensure data security, which led to the disclosure of, and unauthorized access to, four individuals' personal data.

The fine is the third highest issued by Romania under the GDPR.

Spain

Since the beginning of 2021, the Spanish DPA has had noticeable enforcement activity and broke its own personal "highest fine record" multiple times. Generally speaking, the fines issued in the last six months are the highest ever imposed by the Spanish DPA.

- BBVA (*Banco Bilbao Vizcaya Argentina*) - 11 December 2020

The Spanish DPA, the AEDP, issued a fine of €5 million against BBVA for breach of article 13 (obligation of information) and article 6 (legal basis for processing) of the GDPR.

The AEDP highlighted that BBVA used imprecise terminology regarding its privacy policy and provided insufficient information about the category of personal data processed. Furthermore, BBVA failed to obtain consent before sending promotional messages to customers and had not set out a specific mechanism for consent to be obtained. The data processing was thus not based on a freely given, specific, informed and unambiguous consent.

This was, at the time, the largest fine handed out by Spain under the GDPR.

- Caixabank - 13 January 2021

The AEDP imposed a €6 million fine on Caixabank, a financial services company, for processing its customers' data without obtaining their consent.

Similarly to the BBVA case, the company was sanctioned for not providing consistent information across different documents, using imprecise terminology in its privacy policy, and providing insufficient information about the category of personal data processed, the legal basis of processing, as well as the existence of data subjects' rights.

A little more than a month after the BBVA decision, and yet for similar unlawful practices, the AEDP issued a new record breaking fine under the GDPR.

- Vodafone Spain - 11 March 2021

The company received four fines of a total amount of €8.15 million, for violations of the GDPR and Spanish domestic law on data privacy.

The fine resulted from 191 separate complaints against Vodafone**'**s marketing activity from people who had explicitly revoked their consent regarding the processing of their data for advertising purposes. The inspection carried out by the AEDP revealed that Vodafone had not taken sufficient organizational measures to ensure it was processing people**'**s personal data lawfully, and especially to avoid advertising activity aimed towards citizens who had exercised their rights of opposition or erasure of their personal data.

To this day, this is the highest fine ever handed out by Spain.

- EDP Energia - 4 May 2021

The company received a €1.5 million fine for violations of the GDPR. First of all, the fine was imposed because the company failed to obtain valid consent for direct marketing activities. Furthermore, the AEPD noted that the company had failed to implement the principles of "data protection by design and by default."

This case is a more recent example of the AEDP's enforcement activity, and is also the fourth highest fine ever handed out by Spain under the GDPR.

Sweden

- Multiple healthcare providers - 3 December 2020

Heavy fines were imposed on seven healthcare providers audited by the Swedish DPA, for a total amount of 69.5 million of Swedish kronor (approximately €6.9 million).

The DPA identified diverse violations relating to data security, especially in the context of health data processing. More specifically, the Swedish DPA noted that the health care providers had not carried out a needs and risk analysis, as required in order to assign an adequate access authorization to personnel for processing the data contained the electronic health records. According to Magnus Bergström, the coordinator of the audits, "*Without such analysis health care providers cannot assign the personnel a correct level of authorization, which in turn means that the organizations cannot guarantee patients' right to privacy protection*."

This is the second highest fine ever imposed by the Swedish DPA, next to a €7 million fine imposed on Google in March 2020.

United Kingdom

- British Airways - 16 October 2020

The transport company received a fine of approximately 22 million euros (£20 million) for failure to protect the personal and financial details of more than 400,000 of its customers.

The ICO found that the company was processing a significant amount of personal data without adequate measures in place to ensure data security. As a result, the airline was subjected to a cyber-attack during 2018, which was not detected for 2 months.

- Marriott - 30 October 2020

The company received a fine of approximately €20 million (£18 million) for failure to protect the personal and financial details of its customers.

It is estimated that 339 million guest records worldwide were affected by a cyber-attack in 2014. The attack remained undetected until September 2018. The compromised data involved names, email addresses, phone numbers, unencrypted passport numbers, arrival/departure information, guests' VIP status and loyalty program membership number.

The British Airways and Marriott decisions are of significant importance for two reasons.

First of all, they are the highest fines ever issued by the British DPA. It is also worth noting that the intended fines for British Airways and Marriott International were respectively of £183 million and of £99.2 million. However, intended fine may be reduced by DPAs, as they may take into consideration factors such as the development of an action plan to show how the problem will be solved, a commitment to increasing the level of data protection, or even the financial impact of the COVID-19 crisis.

Second, these decisions represent a solid illustration of the tendency of DPAs to work together, when a data breach presents a transnational aspect. In application of the "one-stop-shop" mechanism set out by the GDPR, the decisions drafts got to be examined and approved by other DPAs such as the French CNIL.

- American Express - 5 March 2021

The ICO issued a fine of approximately €105,000 (£90,000) against American Express for failure to collect proper consent before processing data for marketing purposes. During a 12-month period, more than 4 million direct marketing messages were sent by American Express Services Europe Limited. These messages contained direct marketing material for which subscribers had not provided consent