Bloomberg Law

Professional Perspective

Lessons Learned from Key GDPR Enforcement Cases

David Dumont, Anna Pateraki, and Laura Leonard, Hunton Andrews Kurth

Lessons Learned from Key GDPR Enforcement Cases

Contributed by David Dumont, Anna Pateraki, and Laura Leonard, Hunton Andrews Kurth

"GDPR enforcement will increase" is a phrase we have heard many times since the EU General Data Protection Regulation became applicable on May 25, 2018. One of the major innovations of the regulation is the power of EU data protection authorities (DPAs) to impose significant administrative fines for data protection infringements that may amount up to €20 million or 4% of a company's annual worldwide turnover of the preceding year, whichever is greater.

The GDPR's second anniversary is a good time to reflect on what enforcement trends have developed in practice. This article summarizes the key lessons learned from enforcement actions taken by DPAs through May 2020. It is supported by a country-by-country Schedule of important cases that analyzes, for each case, the relevant facts, legal issues, and enforcement outcomes.

In the first months after the GDPR became applicable in 2018, the wave of enforcement actions that some had feared did not materialize. At that time, DPAs—like many companies—were presumably still in the process of adapting to the new legal framework. In 2019, the DPAs settled into their new roles, and enforcement started to pick up significantly. This trend toward more frequent and intense enforcement continued into the first half of 2020, demonstrating that GDPR fines are here to stay.

Based on the enforcement cases discussed in more detail in the Schedule of this article, a number of important lessons can be learned from the first two years of GDPR enforcement in countries like Austria, Belgium, France, Germany, UK, and other EU jurisdictions.

Privacy Notices and Consent Practices

Unsurprisingly, privacy notices and consent practices are often in the scope of DPA investigations. These issues draw particular attention, as these aspects of a company's data protection compliance program are some of the most visible to both regulators and the public. GDPR enforcement decisions have shown the importance of continuously evaluating whether an organization's privacy notices and consent practices are up-to-date and meet the conditions set forth in the GDPR and relevant DPA guidance.

Not only are privacy notices and consent practices important elements of any data protection compliance program, enforcement cases also show that these issues have been key elements of compliance related to direct marketing issues. For example, in France, the DPA imposed a €50 million fine on Google for data protection violations regarding transparency and legal basis issues. It also levied a fine of €500,000 on Futura Internationale, a medium-sized construction company, for multiple GDPR violations in connection with direct marketing, including failure to honor the customer's objection to receiving calls from the company and to provide sufficient notice that the calls were recorded.

Furthermore, in Italy, the DPA fined TIM S.p.A., a telecommunications company, with €27,802,946 for several GDPR infringements, including in connection with the company's consent practices in the context of direct marketing. Similar fines regarding transparency and legal basis issues were identified in Austria, Belgium, France, and the Netherlands.

Data Minimization and Storage Limitation

Data minimization and storage limitation issues are frequently recurring topics in DPA enforcement decisions. As such, organizations should focus on their data retention practices and promptly delete unnecessary personal data. Proper data hygiene is not only essential to ensure compliance with the GDPR's key data protection principles of data minimization and storage limitation, but it also reduces risks related to information security issues.

For example, the importance of data minimization shows in the *Futura Internationale* case in France, where the relevant GDPR violations included that the company maintained excessive comments about customers in its CRM software. In Germany, the €14,500,000 fine imposed on *Deutsche Wohnen SE* highlights the important of the storage limitation principle. The decisive factor for the enforcement action was that the company was retaining personal data for years without verifying whether storage was still necessary.

Security

Implementing and maintaining appropriate technical and organizational information security measures have shown to be crucial elements in GDPR enforcement cases. In practice, information security incidents and the related data breach notification obligations under the GDPR are often the trigger for a DPA investigation.

However, even in cases where an investigation is not initiated due to an information security incident, DPAs typically review the company's information security infrastructure and the associated underlying risk assessment. Data security issues arise in numerous cases that the DPAs investigate, for example, in the existing cases in France (*Sergic*, *Active Assurances*), Germany (*1&1 Telecom GmbH*), Ireland (*Tusla*), Netherlands (*Haga Hospital, Uitvoeringsinstituut Werknemersverzekeringen*), and the UK (British Airways, Marriott International).

Data Subject Rights

The GDPR has also strengthened the rights of individuals with respect to the processing of their personal data and increased public awareness around long-existing data protection rights in the EU. Current DPA enforcement cases demonstrate the importance of having in place robust processes to evaluate and respond to data subject rights requests in a timely manner.

Not doing so is a common source of complaints to a DPA, which in turn, may lead to an investigation. Such data subject rights issues have been highlighted, for example, in the *Futura Internationale* case in France, which related to the right to object to direct marketing activities; the *Delivery Hero* case in Germany, which related to the rights of access, deletion, and objection; and the *Google LLC* case in Sweden where the DPA fined the company €7 million for alleged non-compliance with the GDPR's right to be forgotten.

Cooperation in DPA Investigations

Many enforcement cases described later in this article started with a complaint from a data subject about one specific violation of the GDPR. But once a DPA starts investigating an issue, it may find other data protection compliance gaps. Recent enforcement cases demonstrate that DPAs tend to impose higher fines if their investigations reveal multiple GDPR violations.

In light of this, accountability has proven to be of utmost importance in demonstrating compliance. Often, cooperating with a DPA in the initial stage of an investigation is likely to reduce enforcement risks by, for example, responding promptly to questions concerning the setup of the company's data protection compliance program and being in a position to provide documentation supporting the company's compliance decisions.

A significant number of cases indicate that how a company cooperates with a DPA will be taken into account in determining the level of fine. These include, for example, the *Futura Internationale* case in France, the *Proximus SA* case in Belgium, the *Deutsche Wohnen SE* and the *1&1 Telecom GmbH* cases in Germany, and the *British Airways* case in the UK.

Remediation Measures

If a DPA deems a company's approach to not meet the GDPR standard, the company will be requested or ordered to implement measures to remedy one or multiple violations. This has been evident in the *1&1 Telecom GmbH* and *Deutsche Wohnen SE* cases in Germany, the *Active Assurances* case in France, the *British Airways* case in the UK, and the *Eni S.p.A.* and *TIM S.p.A.* cases in Italy.

We learn from these cases that it is important to implement promptly the measures requested or ordered by a DPA. This will often require the involvement of different teams within the company that need to cooperate closely to develop, execute, and monitor an effective remediation plan.

In practice, DPAs follow-up on their recommendations or orders within a timeframe they find reasonable for the particular case so they can determine whether the company's remediation steps are satisfactory. If a company is not able to demonstrate that it has taken the necessary measures or, at the very least, has a remediation plan in place, this may trigger DPAs to use their sanctioning powers.

Duration of the Violation

In addition to a company's willingness to cooperate with a DPA and comply with its recommendations or orders, the duration of the violation has shown to be an important factor considered by DPAs when making enforcement decisions (see, for example, the *Eni S.p.A.* case in Italy and the case involving an insurance company in Belgium).

Some of the recent enforcement cases demonstrate that continued infringements or infringements of a structural nature will likely be treated with more scrutiny than one-off issues or vulnerabilities that were identified and remedied promptly.

Enforcement of Cookie Consent Issues

In the EU, the use of cookies is regulated by the e-Privacy Directive, which requires the users' informed consent to drop cookies and similar technologies on a user's device, except for strictly necessary cookies, which can be dropped without consent. However, to the extent that the use of cookies involves personal data, the cookie informed consent requirement under the e-Privacy Directive must meet the notice and consent standards of the GDPR.

At the time of the GDPR's two-year anniversary, cookie enforcement was still at an early stage, but the first enforcement cases started to emerge. In Belgium, the DPA imposed a €15,000 fine on a legal news website for non-compliance with several provisions of the GDPR and the e-Privacy Directive, including violations in respect of cookie transparency and consent issues.

In addition, the regulatory environment was not ripe to enforce cookie consent issues shortly after the GDPR became applicable. On the one hand, the DPAs required time to issue guidance and clearly articulate the correlation between the e-Privacy Directive's cookie consent requirements and the provisions of the GDPR.

On the other hand, there were hopes that the relationship between these two laws in respect of cookie issues would be addressed by the EU legislator in the upcoming e-Privacy Regulation, which will replace the e-Privacy Directive.

While the timing for the adoption of the draft e-Privacy Regulation remains uncertain, many DPAs in the EU (e.g., Belgium, Denmark, France, Germany, Greece, Ireland, Italy, Spain, UK) have issued guidance on the use of cookies. In addition, some DPAs made statements that they will seek to enforce their guidance, such as the DPAs in France, Ireland, and the UK. As DPAs focus on cookie issues, we expect enforcement action with regard to cookie issues to increase in the future.

Outlook

Although DPAs were not ready to use their strengthened enforcement powers from the first months that the GDPR became applicable, they have now established themselves and seem to focus on enforcement where necessary.

The lessons learned highlighted in this article are aimed at helping organizations better address challenges in connection with their data protection compliance programs and avoid complaints or investigations, as GDPR enforcement is expected to scale up in the foreseeable future. Importantly, a number of cases during the first two years of the GDPR already resulted in multi-million euro fines–and there seems to be a trend toward this level of fines going forward..

SCHEDULE
Overview of Significant Fines by Country through the GDPR's Second Anniversary

This section provides a high-level overview of selected DPA enforcement cases that resulted in significant administrative fines in the two years since the GDPR became applicable. The list is not exhaustive but highlights the most important issues that organizations should consider moving forward.

AUSTRIA

In 2019, GDPR enforcement in Austria was rather active with several enforcement actions taken by the Austrian Data Protection Authority. In the vast majority of the cases, the DPA decided to take corrective measures, such as ordering deletion of the data or requesting amendments to privacy notices, instead of imposing administrative fines. However, there was one case for which the DPA imposed a multi-million euro fine for non-compliance with data protection principles.

Őesterreichische Post AG

On Oct. 29, 2019, the DPA fined the national postal service Österreichische Post AG €18 million for multiple GDPR violations. Following a complaint by a data subject and revelations in the press, the DPA investigated the company and established that it unlawfully processed information regarding its customers' alleged political affiliations.

In some cases, the company had sold this information to political parties for advertising purposes. Another GDPR violation related to the company's further processing of customer data, including the customers' preferences, habits, package delivery frequency, and frequency of relocations, for direct marketing purposes. The DPA took the position that the processing of personal data for these purposes required the data subject's consent and that, in the absence of such consent, the organization did not have a valid legal basis for its data processing activities..

BELGIUM

In Belgium, GDPR enforcement had a slow start, as members of its Data Protection Authority's executive committee, including the president of the Litigation Chamber, were not appointed by the Belgian Parliament until March 28, 2019. Since the reorganization of the Belgian DPA, however, the litigation chamber has been rather active, with an increasing number of cases resulting in administrative fines at the end of 2019 and beginning of 2020.

In a statement released for the second anniversary of the GDPR, the DPA indicated that it had conducted more than 100 investigations and imposed 59 sanctions, including nine fines totaling €189,000, between May 2019 and May 2020. The agency also indicated that it was in the process of renegotiating its annual budget to be able to handle the increasing number of cases received and conduct large investigations focusing on specific topics or sectors..

Legal News Website

On Dec. 17, 2019, the DPA imposed a €15,000 fine on a company that hosts a legal news website for non-compliance with several provisions of the GDPR and the ePrivacy Directive (Decision 12/2019). With respect to the company's GDPR infringements, the DPA found that the company failed to provide sufficient information to website visitors about the processing of their data and the use of cookies.

Furthermore, the DPA considered that the company's posting of a privacy policy only in English for a website whose audience is mainly Dutch and French-speaking did not meet the level of transparency required by the GDPR. In its decision, the DPA also confirmed that the use of pre-ticked boxes is not a valid mechanism to obtain consent for the use of cookies.

Proximus SA

On April 28, 2020, the DPA imposed a €50,000 fine on the telecommunications company Proximus SA for non-compliance with the GDPR requirements related to the appointment of a data protection officer (Decision 18/2020). According to the DPA, by appointing the head of the compliance, risk management and audit department as a data protection officer, the company had failed to ensure that its data protection officer is free from any conflict of interest in this particular case.

In its decision, the DPA found that a head of a department cannot exercise the role of data protection officer where that function has decision-making powers regarding important data processing activities, as the combination of the two roles in such case is likely to result in a conflict of interest. The DPA's investigation also focused on the duty to cooperate with the DPA and the company's accountability obligations, although the actual fine was imposed for non-compliance with the GDPR's DPO requirement.

Insurance Company

On May 14, 2020, the DPA levied a €50,000 fine on an insurance company, for infringing multiple requirements of the GDPR, including transparency requirements and lawfulness principle. (Decision 24/2020). The decision followed from a complaint filed by a customer regarding the processing of his personal data, including sensitive personal data. The company collected his data for the purpose of hospitalization insurance, but also processed the data for other purposes without properly informing him and giving him a choice about the additional processing purposes.

The insurance company's privacy notice listed several processing purposes—conducting tests, training personnel, performing quality checks, fraud monitoring and prevention, maintaining statistics, and sending marketing communications about the insurance provider's and other companies' products and services—noting that the company relied on the legitimate interests legal ground for processing.

However, the DPA took the view that, except for fraud monitoring and prevention and for direct marketing, the insurance company did not demonstrate a legitimate interest in the processing for its listed purposes, and, therefore, specific consent should have been obtained. In addition, the DPA concluded that the privacy notice of the insurance company did not meet the transparency requirements of Article 13 of the GDPR.

The reasons for this conclusion were, among others, that the privacy notice did not clearly distinguish the purposes for which the company processed sensitive personal data, describe the legitimate interests pursued with the data processing, and list the legal ground(s) for sharing the data with third parties. The DPA further indicated that the insurance company did not clearly inform data subjects about their right to object to the processing of their personal data, including objecting to the data processing for direct marketing purposes. In imposing the fine, the Belgian DPA took into account the gravity and duration of the infringements..

Social Media Provider

On May 14, 2020, the Belgian DPA imposed a €50,000 fine on a social media provider for unlawful processing of personal data in connection with the "invite-a-friend" function offered on its platform (Decision 25/2020). The functionality consisted of collecting and storing personal data of members' contacts to send invitations to connect on the platform. According to the DPA, the social media provider did not have a valid legal ground for the processing of personal data in connection with the "invite-a-friend" functionality, as it was not collecting consent from the members' contacts directly.

In addition, the DPA found that the social media provider did not have an alternative legal ground under the GDPR to legitimize the processing of members' contacts' data. The legitimate interests legal basis was not applicable according to the DPA, as the collection of the members' contacts' personal data was not limited to what was strictly necessary to send invitations and the data was not deleted promptly when it was no longer necessary. Lastly, the DPA found that users were presented with pre-ticked boxes to invite contacts, which did not meet the consent requirements under the GDPR.

FRANCE

In France, the Data Protection Authority (CNIL) has been particularly active. In its Annual Activity Report for 2019, the CNIL revealed a 27% increase of the number of complaints received in 2019 compared to 2018, and a 79% increase in the last five years. The number of investigations conducted by the CNIL remains high, with 300 investigations conducted in 2019.

Overall, the CNIL imposed eight sanctions in 2019, including seven fines totaling €51,370,000, and five additional injunctions subject to a financial penalty. On March 17, 2020, the CNIL released its annual inspection program, announcing that inspections for 2020 will focus on the security of health data processing activities, geolocation for community or proximity services, and the use of cookies and similar technologies. Below is a summary of the key fines imposed by the CNIL to date.

Google LLC

On Jan. 21, 2019, the CNIL imposed a record €50 million fine on Google LLC following complaints filed by two non-profit associations on May 25, 2018, and May 28, 2018, respectively (Délibération n°SAN-2019-001). The company was fined for alleged data protection violations regarding transparency and legal basis. One of the complaints alleged that mobile phone users of Google's Android operating system were required to accept Google's privacy policy and general terms of use in order to use their mobile phones, but the company did not provide notice in an easily-accessible form using clear and plain language when users configured their Android mobile devices.

The other complaint alleged that the company did not obtain users' valid consent to process their personal data for ad personalization purposes. In its ruling, the CNIL established that the company's disclosures were not easily accessible for users and that information was spread between several documents, requiring the user to click multiple buttons and links to access additional information about the data processing. In addition, the CNIL was not satisfied with several references in the company's privacy policy, including the description of the purposes of the data processing, the types of data processed, the legal basis for the data processing, and retention issues.

With respect to the consent issues, in CNIL's view, the users' consent for ad personalization was not sufficiently:

- Informed, because information was diluted across several documents
- Unambiguous, because the company used pre-checked boxes in the account settings to display personalized ads, revealing the lack of clear affirmative action by the user
- Specific, because at the time of creating an account, the users were asked to consent to all processing operations described in the company's privacy policy and not distinctly to each purpose

A determining factor for the amount of the fine was, among others, that the alleged GDPR violations were continuous, despite the measures implemented by the company. The company claimed that the CNIL did not have jurisdiction, as the company's main establishment is located in Ireland, but the CNIL took the position that the GDPR's one-stop mechanism did not apply in connection with the data processing activities addressed by the complaints. Google's appeal of the CNIL's decision before the French Council of State was rejected in a decision dated June 19, 2020.

Futura Internationale

On Nov. 21, 2019, the CNIL imposed a fine of €500,000 on a medium-sized construction company Futura Internationale, for multiple GDPR violations in connection with processing personal data for direct marketing purposes (Délibération No. SAN-2019-010). A data subject complained to the CNIL that she was contacted regularly by the company for direct marketing purposes despite the fact that she had objected to receiving calls from the company.

The CNIL investigated the issue and established that the company had failed to:

- Honor individuals' objections to the processing of their personal data for direct marketing purposes
- Comply with the data minimization principle because excessive comments about customers were maintained in the company's CRM software, including comments in relation to customers' health conditions
- Provide sufficient notice regarding the recording of customers' phone calls
- Implement an appropriate data transfer mechanism for the transfer of personal data to call center vendors based outside the EU

In addition, the CNIL stated that the company had not cooperated with the CNIL in a satisfactory manner after the authority issued a formal notice against the company requesting the company to take corrective measures to remedy the violations.

Sergic

On May 28, 2019, the CNIL levied a fine of €400,000 on real estate company Sergic for a personal data breach, including failure to implement appropriate technical and organizational information security measures and data retention violations. (Délibération n°SAN-2019-005). A user of Sergic's website complained to the CNIL that he was able to access housing documents of others when logged in to his account, by slightly modifying the URL displayed in the browser. The CNIL verified the issue online and established that documents sent by applicants for rental purposes could be freely accessed by others, without prior authentication.

The types of data that were accessible in these documents included copies of ID cards, social security cards, tax notices, certificates issued by the family allowance fund, divorce judgments, account statements, and bank accounts. Furthermore, the CNIL established that the company was aware of this vulnerability six months before the complaint was filed.

During this period, the company had initiated measures to correct the vulnerability but was only able to finalize them a few days after it was informed by the CNIL that this vulnerability constitutes a data breach. When looking into this issue, the CNIL also found that the company was keeping all documents of unsuccessful rental candidates in an active database for an indefinite period, and that it had failed to define and implement appropriate data retention periods for this data.

In the CNIL's opinion, personal data of unsuccessful rental candidates should not have been retained in an active database for more than three months after the housing was allocated. The initial fine proposed by the CNIL was €900,000, which was reduced to €400,000 after considering more closely the size of the company and its financial capacity.

Active Assurances

On July 18, 2019, the CNIL fined insurance company Active Assurances €180,000 for similar reasons as those in the data breach described above (Délibération n°SAN-2019-007). Following a complaint and an online investigation, the DPA established that customer documents were accessible online simply by changing the numbers at the end of the URL in the browser. The documents included copies of driver's licenses, vehicle registration documents, and bank statements.

In addition, the authority was notified that customer accounts were accessible without prior authentication through links on search engine results. The CNIL alerted the company, and the company took corrective measures; however, the authority was not satisfied with those measures. The CNIL considered the small-to-medium size of the company when levying the fine.

GERMANY

Enforcement increased rapidly in Germany in 2019, resulting in multi-million euro fines for GDPR violations. This increase likely relates to a specific fining model that German DPAs follow, which is generally expected to result in high GDPR fines. In addition, despite an increase in staff and budget, the majority of the German DPAs found that current staffing and financial resources are not sufficient to allow an adequate and proactive fulfillment of their statutory tasks.

Deutsche Wohnen SE

On Nov. 5, 2019, the Berlin Data Protection Commissioner announced a fine of €14,500,000 on real estate agency Deutsche Wohnen SE, for failure to comply with the data storage limitation principle of the GDPR. According to the authority's press release, the underlying violation was that the company's data storage system did not include a functionality to delete personal data of tenants that was no longer necessary for the purpose for which the data was initially collected.

The press release highlighted that the company was retaining personal data for years without verifying whether storage was still necessary. As a result, financial, employment, social security, tax, and health insurance information could be accessed. The authority required the company to change its data storage system and bring its data retention practices into compliance with the law, but over one year later, the authority found that the measures the company had taken were not sufficient.

Because the company's turnover of the preceding year was more than €1 billion, the authority stated that the company should have been fined approximately €28 million. However, the authority took into account that the company took initial measures to remedy the violation and cooperated with the authority, as well as that there was no evidence of unauthorized access to the retained data. Ultimately, the authority imposed a €14 million fine "in the middle for the initial fine range.".

1&1 Telecom GmbH

On Dec. 9, 2019, the German Federal Data Protection Commissioner fined telecom provider 1&1 Telecom GmbH €9,550,000 for violating data security through insufficient technical and organizational measures to secure personal data. According to the authority's press release, the company's customer service group used insufficient authentication procedures, which resulted in callers being able to obtain extensive information about customers of the company simply by providing the customer's name and date of birth.

The authority took the position that the authentication procedure, as it was set up, did not comply with the GDPR's data security requirements. The company started requesting additional information to verify the identity of the callers, and worked on introducing an improved authentication procedure in consultation with the authority.

Despite these mitigation measures, the authority deemed it was necessary to impose a fine because the inadequate initial authentication process represented a risk for the entire customer base of the company. But because the company cooperated with the authority, the fine that was ultimately imposed was "at the lower end" of the range, according to the authority.

Delivery Hero Germany GmbH

On Sept. 19, 2019, the Berlin Data Protection Commissioner announced fines totaling €195,407 on food-delivery service Delivery Hero Germany GmbH for various GDPR violations, focusing on non-compliance with requests of data subjects exercising their rights of access, deletion and objection. According to the authority's press release, the company had not deleted online customer accounts in 10 cases, even though these customers were inactive for years, with one inactive since 2008.

In addition, eight former customers had complained about receiving unsolicited advertising e-mails from the company. One person had expressly objected to the use of his data for advertising purposes, but still received 15 advertising e-mails from the company. In five other cases, the company either did not respond promptly to access requests of customers or responded only after the authority received a complaint.

The authority emphasized that any company processing personal data must implement technical and organizational measures that allow the processing of data subject rights requests without undue delay. The company explained to the authority that some of the GDPR violations were due to technical errors or employee oversight, but the authority took the position that the human error coupled with the high number of repeated violations revealed fundamental, structural and organizational issues at the company.

Hospital

€105,000 fine for non-compliance with data protection principles. On Dec. 3, 2019, the Data Protection Commissioner of the federal state Rhineland-Palatinate announced a €105,000 fine against a hospital for several violations of GDPR data protection principles related to poor technical and organizational measures for the processing of patient data, which resulted in the incorrect invoicing of a patient. The authority stated that due to the sensitivity of health-related personal data, data protection authorities are particularly vigilant regarding data processing in the health-care sector—a concept reinforced by this fine.

The German data protection authorities issued more than 200 administrative fines under the GDPR in the period from the enactment of the GDPR in May 2018 until the end of 2019. The authorities in the majority of these enforcement cases indicated that the actual amount of the fine imposed took into account the size of the company.

UNITED KINGDOM

Before Brexit, the UK Information Commissioner's Office issued only one fine under the GDPR. The ICO also exercised its other enforcement powers and issued several enforcement notices. In addition, the agency issued intentions to fine that could potentially result in the highest fines imposed throughout the EU since May 2018. These fines, however, are have not been confirmed and they could be subject to adjustment. Below is a summary of the ICO's key fine and intentions to fine under the GDPR to date.

British Airways

On July 8, 2019, the ICO announced its intent to impose a £183,390,000 fine on British Airways for failure to implement appropriate security measures to protect customer data, which resulted in a breach affecting approximately 500,000 customers that was notified by British Airways to the ICO. As a result of the breach, personal data, such as payment cards, travel booking names, addresses and log-in details, was harvested. The ICO investigated the breach under the GDPR's one-stop mechanism, and when determining the fine it took into account the steps that the company took to mitigate the impact of the breach and address the underlying security issues, as well as the fact that the company cooperated with the ICO during the investigation. As of July 2020, the amount of the fine was not yet final.

Marriott International, Inc.

On July 9, 2019, the ICO announced its intention to impose a £99,200,396 fine on Marriott International, Inc. following a cyber-incident that was notified to the ICO in November 2018. The data breach involved approximately 339 million guest records, including 30 million records related to residents of the European Economic Area, and 7 million UK residents. The vulnerability began when systems of the Starwood hotels group acquired by Marriott were compromised. The ICO took the position that the company failed to undertake appropriate due diligence during the Starwood acquisition and should have taken additional measures to protect its systems. As of July 2020, the amount of the fine is not yet final.

Doorstep Dispensaree Ltd

On Dec. 20, 2019, the ICO levied a £275,000 fine on Doorstep Dispensaree Ltd, a London-based pharmacy, for failure to ensure the security of sensitive personal data. The company had left approximately 500,000 documents containing sensitive personal data of customers, such as identification data, date of birth, medical information, prescriptions and NHS numbers, in unlocked containers at the back of its premises..

OTHER EU COUNTRIES

Overall, enforcement actions across the EU show an increased attention and effort toward enforcement by most EU DPAs. See Contribution of the EDPB to the evaluation of the GDPR under Article 97 (adopted Feb. 18, 2020). Between May 2018 and the end of November 2019, 22 EU DPAs had used their corrective powers, issuing approximately 785 fines altogether. Only eight EU DPAs had not yet imposed administrative fines by the end of 2019.

IRELAND

The Irish Data Protection Commission imposed its first fine for GDPR violations on May 17, 2020. The fine was imposed on Tusla, Ireland's Child and Family Agency, following an investigation started at the end of 2019 concerning three data breaches. Following its inquiry, the Irish DPA found that the data breaches involved the contact details and location data of a mother and child of an alleged abuser, as well as data about children in foster care. The authority also conducted a significant number of investigations into technology companies in 2019, and is expected to render decisions, and potentially impose administrative fines, in a number of these enforcement cases in 2020.

ITALY

The DPA (Garante) also recently started to impose high fines. On Dec. 11, 2019, for example, the agency imposed two fines totaling €11,500,000 on the oil and gas company Eni S.p.A. for unlawful processing of personal data in the context of promotional activities and the activation of unsolicited contracts. In imposing the fine, the Garante took into account the wide range of stakeholders involved in the infringement, the pervasiveness of the conduct, duration of the infringement, and the economic conditions of the company. The Garante also ordered Eni to take several corrective measures.

Approximately a month later, the Garante imposed a €27,802,946 fine, as well as several corrective measures, on the telecommunications company TIM S.p.A. for unlawful data processing activities in connection with the company's marketing practices. The DPA identified a number of GDPR infringements, including insufficient monitoring of call centers hired to make marketing calls on TIM's behalf, failure to update the list of individuals who had opted-out of receiving marketing communications and making consent to marketing communications a condition for customers to receive discounts and participate in sweepstakes..

NETHERLANDS

The Netherlands has also seen an increase in GDPR enforcement cases. On June 28, 2019, the Dutch DPA imposed a fine of €460,000 on health-care provider Haga Hospital for a failure to implement appropriate technical and organizational measures, including insufficient authentication controls for access to medical records. In October 2019, the DPA also sanctioned the Dutch employee insurance service provider Uitvoeringsinstituut Werknemersverzekeringen for not implementing appropriate information security measures.

The DPA found that the insurance service provider did not use multi-factor authentication to protect access to its online employer portal, which the DPA considered vital given the sensitivity of personal data stored on the portal. The portal stored health data, including data related to employees' absenteeism. In this case, the DPA decided to impose a fine of €150,000 per month that the violation continued, with a maximum of €900,000, instead of a one-time amount.

In Nov. 2019, the insurance service provider requested and obtained a suspension of the sanction until March 1, 2020. In another case, on March 3, 2020, the DPA fined the Royal Dutch Tennis Association €525,000 for illegal sale of the personal data of more than 350,000 of its members. Members of the association had submitted a complaint to the DPA after being informed of the association's intention to provide members' personal data to sponsors for targeted marketing purposes. The authority found that the sale of personal data to the association's sponsors was unlawful because it occurred without a valid legal ground.

On April 30, 2020, the DPA imposed a €750,000 fine on a company for unlawful processing of employees' fingerprints for attendance and time registration purposes. Fingerprints are biometric data, which qualifies as sensitive personal data under the GDPR. The DPA found that the company did not have a legal ground to legitimize the processing of employees' fingerprints and that the use of fingerprints was unnecessary and disproportionate.

SPAIN

Enforcement is also increasing in Spain, particularly since the beginning of 2020. On June 11, 2019, the Spanish DPA fined the national football league, LaLiga, €250,000 for non-compliance with the GDPR's transparency principle (Case No. PS/00326/2018). The case concerned a functionality of the organization's mobile app, which was using smartphone microphones and collecting geolocation information. The authority took the position that additional notice should have been provided to users at the time the processing occurred—meaning every time the device recorded audio and collected geolocation information—through, for example, pop-ups or push notifications.

Between January and March 2020, the DPA imposed several fines on telecommunications operator Vodafone España for several data protection infringements, including unlawful marketing data processing practices, violation of the principles of lawfulness, integrity and confidentiality, and failure to provide information to the DPA within the required timeframe.

The amount of the various fines ranged from €3,000 (in Case No. PS/00445/2019) to €120,000 (in Case No. PS/00235/2019), totaling more than €560,000. The highest fine imposed on the telecommunications operator was imposed for failure to prove that appropriate consent was collected from data subjects, and unlawful sharing of data subjects' personal data with credit reporting agencies..

SWEDEN

Sweden's DPA issued a few fines since the enactment of the GDPR, one of which was a multi-million euro fine. On March 11, 2020, the DPA announced it had imposed a €7 million fine on Google LLC for failure to comply with the GDPR's right to be forgotten. The DPA decided to impose the fine as Google had not properly removed two search result listings, despite being ordered to do so by the authority back in 2017.

The DPA also argued that Google's practice of informing website owners about links removed from search results and the identity of the person who submitted the removal request is unlawful and discourages individuals from exercising their right to be forgotten.