



# The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities

Brian Daigle and Mahnaz Khan

## *Abstract*

The European Union (EU) General Data Protection Regulation (GDPR) was enacted in May 2016 with a two-year implementation period that concluded in May 2018. Since then, EU member states and regional-level data protection authorities (DPAs) have issued over \$500 million in fines. Although EU DPAs issued few fines for noncompliance in the first year of implementation, DPAs have subsequently acted much more aggressively against noncompliant firms. This paper will explore the broad trends in investigation and enforcement across the EU in the 21 months following GDPR implementation. These trends include a preliminary analysis of differences in GDPR enforcement in specific EU member states, the GDPR provisions that are most emphasized in enforcement, and the nature of the fines imposed on U.S. and EU-based firms. As of March 2020, the largest fines and enforcement actions under GDPR had occurred principally in Western European countries, with a split between enforcement against both U.S. and EU firms.

Suggested citation: “The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities.” *Journal of International Commerce and Economics*. May 2020.  
<https://www.usitc.gov/journals>.

The author(s) would like to thank the two anonymous referees for their comments on earlier versions of this paper.

## Introduction

The European Union (EU) General Data Protection Regulation—Regulation (EU) 2016/679 (GDPR)—came into force on May 25, 2018, after becoming law in April 2016. GDPR covers the processing of personal data and the free movement of such data for approximately 500 million data subjects<sup>1</sup> of the EU as well as Norway, Liechtenstein, and Iceland. GDPR governs the behavior of firms and individuals that act as the controllers of personal information as well as the processors<sup>2</sup> of such information. In addition, GDPR lays out guidelines to address necessary measures in the event of data breaches, defines the rights of data subjects with respect to their personal data, and explains the legal framework for firms protecting personal data and receiving consent for its use. GDPR was adopted as a single comprehensive law in order to resolve the fragmented nature of prior data privacy laws that were embedded in different national systems throughout the EU.<sup>3</sup>

This paper explores the reasons certain European countries issued GDPR fines and enforced certain GDPR violations during the May 2018 to March 2020 period. Since GDPR was implemented in May 2018, early trends in enforcement by different EU data protection authorities (DPAs) have been discernable throughout the EU. Although GDPR is a comprehensive data protection and privacy law that applies to all EU member states, some EU members have placed an emphasis on enforcing certain GDPR provisions over others. For example, France's recent enforcement actions suggest that the country places more importance on companies not using personal data for targeted advertising, while the United Kingdom (UK) appears to emphasize punishing companies for failing to adequately protect data or notify customers once personal data have been breached.

In addition, EU member states have issued fines to firms that have violated GDPR, but these fine levels have often varied depending on the country imposing the fine and the specific GDPR violation. In the first year of GDPR implementation, from May 2018 to May 2019, there were

---

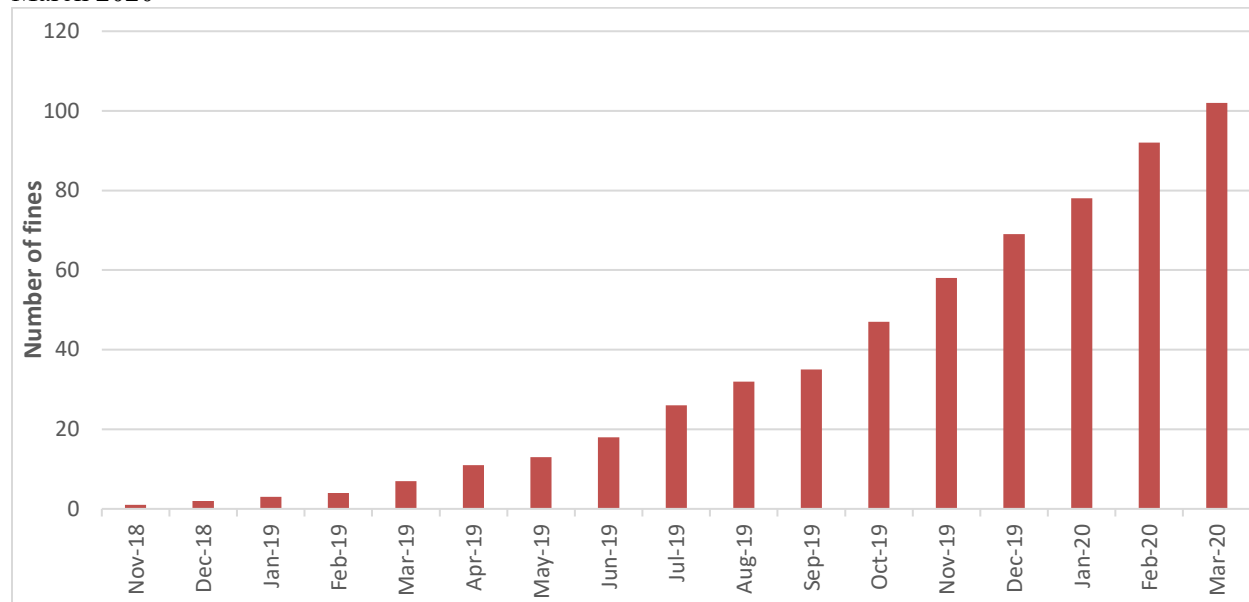
<sup>1</sup> A “data subject” defined under GDPR is any individual (not necessarily an EU citizen) in the territory of the European Union (as well as Norway, Liechtenstein, and Iceland). It means a U.S. citizen who opens a Facebook account in Germany would be covered by the scope of GDPR as a data subject, while a German citizen opening a Facebook account in Brazil would not.

<sup>2</sup> Under the GDPR, controllers are defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Processors are defined as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

<sup>3</sup> EC, “Data Protection in the EU” (accessed September 26, 2019).

fewer than 20 fines issued by all EU DPAs; however, this increased more than fivefold from May 2019 to March 2020 (figure 1).<sup>4</sup>

**Figure 1:** Number of fines issued by EU data protection authorities (DPAs), cumulative, May 2018–March 2020



Note: These data include only fines that are publicly available and that exceed €10,000 (\$10,848).

Source: GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed April 9, 2020).

Two of the three largest fines have been against U.S. firms (discussed in the section “Impact of Enforcement on U.S. Firms”). In many cases, the largest fines have been issued by Western European countries such as France, Italy, and the United Kingdom. For purposes of our analysis, Western Europe will refer to the 18 countries that were in the European Community or European Economic Area before the large 2004 expansion of the EU into the former Soviet and Soviet satellite states. These Western European countries are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, and the UK.<sup>5</sup> Eastern Europe will be defined as the 13 countries that joined the EU in the expansions of 2004, of 2007, or 2013. These countries are Bulgaria, Croatia, Cyprus, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia, and Slovenia.

This paper opens by addressing the history of data protection laws in Europe, how GDPR was adopted, and its current enforcement structure within each EU or EEA<sup>6</sup> member state. Second, it

<sup>4</sup> These data only include fines for which information is publicly available and exceed €10,000. GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed April 9, 2020).

<sup>5</sup> The UK officially exited the EU on January 31, 2020. For the purposes of this paper, the UK will be treated as an “EU member” country, since most of the fines discussed in this paper take place between May 2018 and March 2020.

<sup>6</sup> European Economic Area (EEA) countries are not EU member states but are subject to GDPR. These countries include Iceland, Liechtenstein, and Norway.

explores the most important articles of GDPR in more detail, including those covering (1) general principles related to the legal processing of personal data; (2) the legal basis for data processing, which includes whether a data controller has the authority to process data and whether data processing is lawful; and (3) the circumstances in which a data breach occurred and the possible liability for such breaches. Third, the nature of enforcement actions by the EU DPAs is discussed, illustrating that there are differences in how Western and Eastern European countries are enforcing specific data provisions affecting firms in their respective regions in terms of which companies are being targeted and how fines are distributed. Fourth, a micro-level analysis shows how specific countries are enforcing fines in their own countries including the UK, France, Italy, Germany, the Netherlands, and Ireland. A broad analysis of fines in Eastern European countries is also offered. The final section highlights GDPR's impact on U.S. firms, showing that many of the fines are targeted towards U.S. technology providers or U.S. multinationals offering services in the EU.

## History of Data Protection and Privacy in the EU

GDPR was preceded by two key data protection directives. The first was the 1980 Organisation for Economic Cooperation and Development (OECD) "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (OECD Recommendations on Protection of Privacy)."<sup>7</sup> Updated in 2013, the OECD's seven principles state that (1) individuals should be notified when their personal data are collected, (2) collection should be limited and with the consent of the data subject, (3) data collection should be relevant, up-to-date, and for a specific purpose, (4) data should not be disclosed except with user consent or for legal reasons, (5) data should be protected by security safeguards, (6) data subjects should have the right to have information on what data are collected about them, and (7) controllers of personal data should be accountable for complying with the law.

The second was the 1995 EU Data Protection Directive (Directive),<sup>8</sup> which was built on the seven general principles contained in OECD Recommendations on Protection of Privacy. The Directive governed the regulation of personal data online from 1995 until GDPR was implemented in 2018.<sup>9</sup> The OECD Recommendations on Protection of Privacy, the Directive, and GDPR all contain similar principles regarding data protection and privacy. Specifically, among these principles are the right for data subjects to know what their data are used for, that the data are used with their consent, and that this data is processed for clear and legal purposes. Compared to the Directive and OECD Recommendations, GDPR broadens the rights for data subjects and their access to and

---

<sup>7</sup> Lord, "What Is the Data Protective Directive? Predecessor to the GDPR," September 12, 2018.

<sup>8</sup> Additionally, before 1995, several countries and regional parliaments across the EU had passed their own individual data protection acts. The Hessian parliament in Germany passed a Data Protection Act in 1971, and Sweden created the world's first national data protection legislation in 1973. OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 2013; OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (accessed September 25, 2019); OECD, "Thirty Years After: The OECD Privacy Guidelines," 2011.

<sup>9</sup> The European Data Protection Directive is officially Directive 95/46/EC.

control over the use of their data. Some of these enhanced measures include the subject's rights to be forgotten, to rectify their data, to ensure their data are portable, and to know what the data are being used for.

The main difference between GDPR and its two data protection predecessors is the level of enforceability and the specific enforcement mechanisms that EU members can use to fulfill data protection. The earliest data privacy principles contained in the OECD Recommendations on the Protection of Privacy were purely voluntary for EU countries. The Directive required substantial member state implementing legislation compared to that required by GDPR. The latter, as a European regulation, is fully enforceable at the European level (though it also contains implementing legislation at the member state level and sometimes at the regional level).<sup>10</sup> EU member states under the Directive were allowed to issue fines at their discretion, with no floor or ceiling to these fines.<sup>11</sup> Under GDPR, fines for the most serious violations can reach as high as €20 million (\$22 million) or 4 percent of global turnover (or a firm's worldwide annual revenue), whichever is larger. Certain violations are subject to a lower rate set at 2 percent of global turnover or a €10 million (\$10.9 million) ceiling.<sup>12</sup>

## GDPR Enforcement Structure

Enforcement of GDPR falls under multiple tiers of enforcement that range from regional (in some cases), to the EU member-state level, and up to the broader EU level. Principally, enforcement of GDPR obligations fall under the jurisdiction of EU member states' data protection authorities (DPAs) (table 1). DPAs are appointed by each EU member state, but the number of DPAs within an EU state may vary.<sup>13</sup> For example, some EU members, such as Germany, appoint multiple DPAs within their federal structure (see box 1).<sup>14</sup> However, it is more common for EU members to appoint a single public body that is responsible for enforcing GDPR.<sup>15</sup>

A DPA has significant enforcement powers under GDPR, including the ability to levy substantial fines. A DPA's responsibilities are more broadly defined in GDPR than they were in the

---

<sup>10</sup> OECD, "Thirty Years After: The OECD Privacy Guidelines," 2011.

<sup>11</sup> For example, in October 2018, as a result of the investigation of the firm Cambridge Analytica, the UK's Information Commissioner's Office (ICO) fined Facebook £500,000 (\$618,000) for failing to protect user data. This fine represented the maximum fine that could be issued under UK law under the data protection framework that was in place in the UK prior to GDPR enforcement. Additionally, using legal data protection frameworks that preceded GDPR, the Dutch and UK data protection authorities issued a combined \$1.2 million fine for a data breach at Uber. Waterson, "UK Fines Facebook £500,000 for Failing to Protect User Data," October 25, 2018; Schulze, "Uber Fined Nearly \$1.2 Million by British and Dutch Authorities for 2016 Data Breach," November 27, 2018.

<sup>12</sup> Lower fines at the 2 percent of global revenue (or €10 million) threshold can be issued for infringements by controllers and processors of personal data under GDPR Articles 8, 11, 25–39, 42, and 43. GDPR EU, "Fines and Penalties" (accessed September 26, 2019).

<sup>13</sup> Gabel, "Chapter 14: Data Protection Authorities," April 5, 2019.

<sup>14</sup> Gabel, "Chapter 14: Data Protection Authorities," April 5, 2019.

<sup>15</sup> Gabel, "Chapter 14: Data Protection Authorities," April 5, 2019.

Directive.<sup>16</sup> A DPA handles any issues regarding data breaches reported by a firm, mediates data subject access requests, and provides guidance in interpreting specific GDPR provisions.<sup>17</sup> DPAs also conduct investigations of firms whose headquarters are within their jurisdiction or if data subjects within their jurisdiction are affected by a claim of privacy infringement.<sup>18</sup> However, after implementation of GDPR, there has been some confusion between DPAs about the areas of responsibility. For example, on the issue of jurisdiction, there has been uncertainty as to which EU member country is responsible for conducting an investigation on firms within the EU whose business affects many EU data subjects. Nevertheless, in such situations, DPAs in different EU countries are supposed to collaborate with each other to determine who has the ultimate authority to conduct an investigation.

**Table 1:** List of EU data protection authorities, by country

EU Country	Data Protection Authority	EU Country	Data Protection Authority
<b>Austria</b>	Austrian Data Protection Authority	<b>Latvia</b>	Latvian Data State Inspectorate
<b>Belgium</b>	Data Privacy Commission	<b>Lithuania</b>	State Data Protection Inspectorate
<b>Bulgaria</b>	Commission for Personal Data Protection	<b>Luxembourg</b>	National Commission for Data Protection
<b>Croatia</b>	Personal Data Protection Agency	<b>Netherlands</b>	Dutch Data Protection Authority
<b>Cyprus</b>	Personal Data Protection Commission	<b>Poland</b>	Personal Data Protection Office
<b>Czech Republic</b>	Office for Personal Data Protection	<b>Portugal</b>	National Commission Data Protection
<b>Denmark</b>	Danish Data Protection Agency	<b>Romania</b>	National Authority for the Supervision of Personal Data Processing
<b>Estonia</b>	Data Protection Inspectorate	<b>Slovakia</b>	Office for Personal Data Protection
<b>Finland</b>	Office of the Data Protection Ombudsman	<b>Slovenia</b>	Information Commissioner of the Republic of Slovenia
<b>France</b>	Commission Nationale de L'informatique et Des Libertes (National Commission on Informatics and Liberty)	<b>Spain</b>	Data Protection Agency
<b>Germany<sup>a</sup></b>	Federal Commissioner for Data Protection and Freedom of Information	<b>Sweden</b>	Data Protection Authority
<b>Greece</b>	Hellenic Data Protection Authority	<b>United Kingdom<sup>c</sup></b>	Information Commissioner's Office

<sup>16</sup> Gabel, "Chapter 14: Data Protection Authorities," April 5, 2019.

<sup>17</sup> Buckbee, "GDPR Protection Supervisory Authority Listing," April 8, 2019.

<sup>18</sup> Under Article 77, GDPR complaints can be lodged "with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work, or place of the alleged infringement." GDPR, Article 77. <https://gdpr-info.eu/art-77-gdpr/> (accessed September 25, 2019).

## EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

<b>Hungary</b>	Hungarian National Authority for Data Protection and Freedom of Information	<b>Iceland<sup>b</sup></b>	Data Protection Authority
<b>Ireland</b>	Data Protection Commissioner	<b>Liechtenstein<sup>b</sup></b>	Data Protection Office
<b>Italy</b>	Italian Data Protection Authority (Garante)	<b>Norway<sup>b</sup></b>	Data Protection Authority

Source: Compiled by authors.

<sup>a</sup> Although Germany has a national level data protection authority, most implementation of GDPR falls under the state data protection authorities (box 1).

<sup>b</sup> Norway, Iceland, and Liechtenstein are not EU member states. However, they do belong to the European Economic Area and are subject to GDPR.

<sup>c</sup> The United Kingdom exited the European Union on January 31, 2020.

### Box 1: Germany's Unique Data Supervisory Authority System

Under German law, data protection is a shared responsibility between the German states (*Länder*) and the German federal government. As such, the 16 German states each have their own data protection supervisory authorities and data protection laws, and each authority has state jurisdiction. The national data protection authority, which serves as the German representative to the European Data Protection Board, operates in Bonn.

One of the first verified fines levied by Germany originated in the state of Baden-Württemberg, which imposed a fine on a social media company for failing to implement appropriate data security obligations.<sup>a</sup> The states of Berlin, Hamburg, Saarland, and Sachsen-Anhalt have all been identified as issuing fines for GDPR violations within their jurisdictions. The largest fine in Germany, thus far, was levied by the Data Protection Authority of Berlin in August 2019 on a property rental company, Deutsche Wohnen, in the amount of €14.5 million (\$15.8 million).<sup>b</sup> One survey of firms in Germany estimates that as many as 41 fines were levied by the 16 *Länder* authorities between May 2016 and February 2019.<sup>c</sup>

Industry experts contend that Germany's federal system has likely led to uneven implementation of GDPR across the German states. For example, these experts speculate that local divergences on video surveillance led a federal administrative court to issue a ruling on how video surveillance by private bodies should be governed across Germany.<sup>d</sup>

<sup>a</sup> Schmidt, "Germany's First Fine under GDPR Offers Enforcement Insights," November 27, 2018.

<sup>b</sup> GDPR Enforcement Tracker [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed September 6, 2019)

<sup>c</sup> Schultz, "German Authorities Issue 41 Fines: Report," February 25, 2019.

<sup>d</sup> Runte and Schneider, "Data Law Navigator," July 11, 2019.

At the EU level, the European Data Protection Board (EDPB) was established when GDPR came into effect on May 25, 2018, and the heads of each DPA are members of the EDPB.<sup>19</sup> The EDPB was created to adjudicate conflicting decisions between EU member DPAs, to issue opinions and guidance on particular GDPR provisions, and to oversee that GDPR is being applied consistently

<sup>19</sup> EC, "What Is the European Data Protection Board (EDPB)?" (accessed September 25, 2019).

within the EU.<sup>20</sup> The EDPB also issues binding decisions on disputes about cross-border processing, so that there is consistent application of procedures across various EU jurisdictions.<sup>21</sup>

The EU courts also have jurisdiction in GDPR enforcement. Under GDPR, three judicial bodies—national courts,<sup>22</sup> the European Court of Human Rights (ECHR), and the European Court of Justice (CJEU)—have jurisdiction over disputes that emerge between a DPA and an affected entity,<sup>23</sup> and can define unclear provisions of GDPR.<sup>24</sup> Additionally, at the EU level, officials like the European Advocate General play a role in facilitating the process of moving GDPR complaints through the EU court system.

## GDPR Article Violations

GDPR violations have been categorized by DPAs as occurring under three major articles relating to the legal processing of data and data breaches. According to one source, the most frequently cited article violation was under Article 5, which covers the general principles relating to the legal processing of personal data.<sup>25</sup> A survey of fines, compiled from rulings cataloged by London-based law firm CMS, found that between May 2018 and September 2019, Article 5 was cited in 33 of 73 instances across the European Union where the DPA issued the fine with identifiable article-level explanations for judgments.<sup>26</sup>

Following Article 5, the two most frequently cited articles that were violated and led to fines were Articles 6 and 32. Article 6 covers the actual legal basis for data processing under GDPR (such as the consent principle, which is the most frequently cited basis of violation under that article). Article 32 covers the security of processing, which is largely associated with the

---

<sup>20</sup> EC, “What Is the European Data Protection Board (EDPB)?” (accessed September 25, 2019).

<sup>21</sup> EC, “What Is the European Data Protection Board (EDPB)?” (accessed September 25, 2019); EC, “Communication from the Commission to the European Parliament and the Council: Data Protection Rules as a Trust-Enabler in the EU and Beyond-Taking Stock,” July 24, 2019, 5.

<sup>22</sup> For example, the Austrian Supreme Court ruled in June 2019 that a claimant could file a GDPR complaint in Austria against a firm that was headquartered in Ireland. EPIC, “Austrian Supreme Court: GDPR Lawsuits Can Be Filed Throughout the EU,” June 2019.

<sup>23</sup> For example, in a case between Ireland’s DPA and an Irish national (Case C-434/16), the CJEU ruled that written answers to a test would constitute personal data. Future of Privacy Forum, “Case-Law (CJEU, ECHR, national courts),” n.d. (accessed September 26, 2019).

<sup>24</sup> For example, the European Court of Justice issued a clarification following a request for clarification from the Higher Regional Court of Dusseldorf (Germany) that the operator of a website that features a Facebook “like” button can be ruled to be a joint controller of the personal data of visitors, in conjunction with Facebook. IAPP, “CJEU Releases Judgement on Fashion ID Case,” July 29, 2019.

<sup>25</sup> Article 5 of the GDPR stipulates the 6 principles that allow for lawful processing of personal data. These principles are (1) lawfulness, fairness and transparency; (2) purpose limitations; (3) data minimization; (4) ensuring the accuracy of data; (5) storage limitations; and (6) integrity and confidentiality. Article 6 states the legal basis upon which a data controller may process data, including: consent, performance of a contract, compliance with a legal obligation, vital interest of the data subject, performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and legitimate interest of the controller or by a third-party. Mondschein et. al, “Chapter 5, GDPR in a Research Context,” December 22, 2018.

<sup>26</sup> Authors’ calculations based on a variety of sources, though principally the GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed September 23, 2019).



circumstances around data breaches.<sup>27</sup> In more than 70 percent of the cases judged during this period, at least one of these three articles—5, 6, or 32—was identified as being violated. In many instances, the same ruling determined that either two or all three of these articles were violated.

Many of the enforcement actions taken by EU DPAs mainly addressed whether the data processing was lawful and whether a data controller has the legal authority to process an individual's data under Article 6 of GDPR.<sup>28</sup> The enforcement actions regarding lawful processing included “lawfulness, fairness, and transparency, as well as data minimization.”<sup>29</sup> Industry sources in the legal community indicated that from May 2018 to May 2019, EU DPAs appeared to be less focused on punitive action and more on preventing GDPR violations.<sup>30</sup>

## Nature of Enforcement Actions by EU DPAs

Recent enforcement actions by Western European DPAs suggest that they have been more active than their counterparts in Eastern European countries in issuing GDPR fines (table 2). Examples included actions by the UK's Information Commissioner's Office (UK ICO), Italy's Garante, the 16 German DPAs, and the French Data Protection Authority (Commission Nationale de L'informatique et Des Libertes or CNIL) (table 1).<sup>31</sup> As of March 2020, there have been over 100 fines issued by the various EU DPAs plus those of EEA member states, for a combined value of more than €480 million (\$522 million).<sup>32</sup> However, 5 of these fines issued collectively constituted nearly 90 percent of the total value of all EU GDPR fines from May 2018 to March 2020. The remainder was divided among dozens of other fines (for further information on the fines exceeding €10,000 or \$10,848 in that period, please refer to appendix A).<sup>33</sup>

**Table 2:** Cumulative GDPR fines from DPAs exceeding €10,000 (\$10,848), by country, May 2018 to March 2020

Country	Fines (€)	Fines (\$)	Country	Fines (€)	Fines (\$)
Austria	18,061,000	19,592,844	Latvia	150,000	162,722
Belgium	25,000	27,120	Liechtenstein	---	
Bulgaria	3,138,100	3,404,258	Lithuania	61,500	66,716
Croatia	---		Luxembourg	---	

<sup>27</sup> As of September 2019, Article 6 was cited in 22 cases (30 percent of cases), while Article 32 was mentioned in 15 cases (21 percent).

<sup>28</sup> Cherepanova, “GDPR Enforcement Report (May 2019),” May 14, 2019; Akin & Gump, “A Year of GDPR: Five Recommendations to Help Limit Regulatory Scrutiny,” May 30, 2019.

<sup>29</sup> Cherepanova, “GDPR Enforcement Report (May 2019),” May 14, 2019; GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed September 20, 2019).

<sup>30</sup> Cherepanova, “GDPR Enforcement Report (May 2019),” May 14, 2019.

<sup>31</sup> Akin & Gump, “A Year of GDPR: Five Recommendations to Help Limit Regulatory Scrutiny,” May 30, 2019.

<sup>32</sup> GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed September 20, 2019). Calculations based on author estimates.

<sup>33</sup> These three fines are the UK fines against British Airways (€207.4 million or \$225.6 million) and Marriott (€112.2 million or \$122 million) and the French CNIL fine against Google (€50 million or \$54.4 million).

## EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

Cyprus	24,000	26,035	Malta	---	
Czechia	---		Netherlands	1,825,000	1,979,787
Denmark	375,550	407,402	Norway	270,800	293,768
Estonia	---		Poland	877,730	952,174
Finland	---		Portugal	400,000	433,926
France	51,100,000	55,434,047	Romania	440,056	477,379
German regional DPAs	24,890,407	27,001,486	Slovakia	---	
Greece	715,000	775,642	Slovenia	---	2,068,742
Hungary	141,671	153,687	Spain	1,907,000	
Iceland	20,600	22,347	Sweden	7,053,680	7,651,937
Ireland	---		United Kingdom	319,320,000	346,403,125
Italy	39,440,000	42,785,103			

Source: GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed March 25, 2020).

Recent data trends on actual monetary fines issued by specific EU DPAs illustrate that DPAs in Eastern European countries have implemented both fewer fines and fewer large fines; also, they were generally slower to issue fines than were their Western European counterparts, which may have greater regulatory capacity to enforce GDPR within their respective countries (particularly for multinational firms). Most of these monetary fines levied by Eastern European countries have focused on domestically headquartered firms, small organizations, government agencies, political parties, or banks.

The number of fines by country can be viewed in the maps in figures 2 and 3.<sup>34</sup> Of the total fines issued by EU DPAs during May 2018–March 2020, at least 107 fines exceeded €10,000 (\$10,848) and 35 of those fines exceeded €100,000 (\$108,482). Fines exceeding €10,000 (\$10,848) as well as those exceeding €100,000 (\$108,482) were issued by Western European countries in a majority of cases.<sup>35</sup> Specifically, 78 percent of fines larger than €10,000 and 71 percent of fines larger than

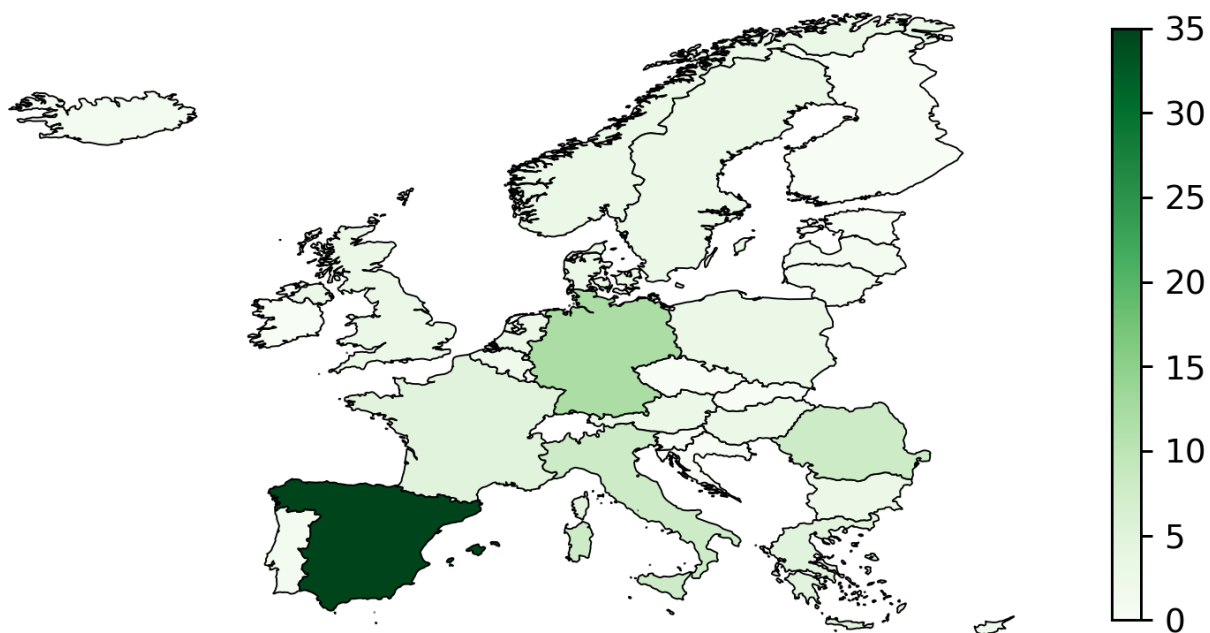
<sup>34</sup> Additionally, appendix B contains a list of fines issued by country and which exceeded €10,000 each, as well as those that exceeded €100,000. Nineteen countries have issued at least one fine that exceeded €10,000, while 12 have not yet issued any fines in excess of €10,000 in this period (though several have issued smaller fines).

<sup>35</sup> Western Europe, for purposes of this analysis, is defined as Austria, Belgium, the Czech Republic, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, and the United Kingdom. Eastern Europe is defined as Bulgaria, Croatia, Cyprus, Estonia, Greece, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia, and Slovenia.

## EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

€100,000 originated from Western European countries.<sup>36</sup> In the case of the former, Spain had issued at least 35 fines in amounts between €10,000 and €100,000 during this period, far higher than any other country. Ten countries have issued at least two fines that exceeded €100,000: Bulgaria, Denmark, France, Germany, Greece, Italy, the Netherlands, Poland, Romania, and the United Kingdom. From May 2018 to March 2020, 11 fines out of more than 100 across the European Union exceeded €1 million each and only 1 was issued by an Eastern European country.<sup>37</sup> Of the 107 fines that exceeded €10,000 each, between May 2018 and March 2020, 26 (24 percent) originated in Eastern European countries and these countries only accounted for 11 percent of EU GDP.<sup>38</sup>

**Figure 2:** EU GDPR fines by country in excess of €10,000 (\$10,848) each, May 2018 – March 2020



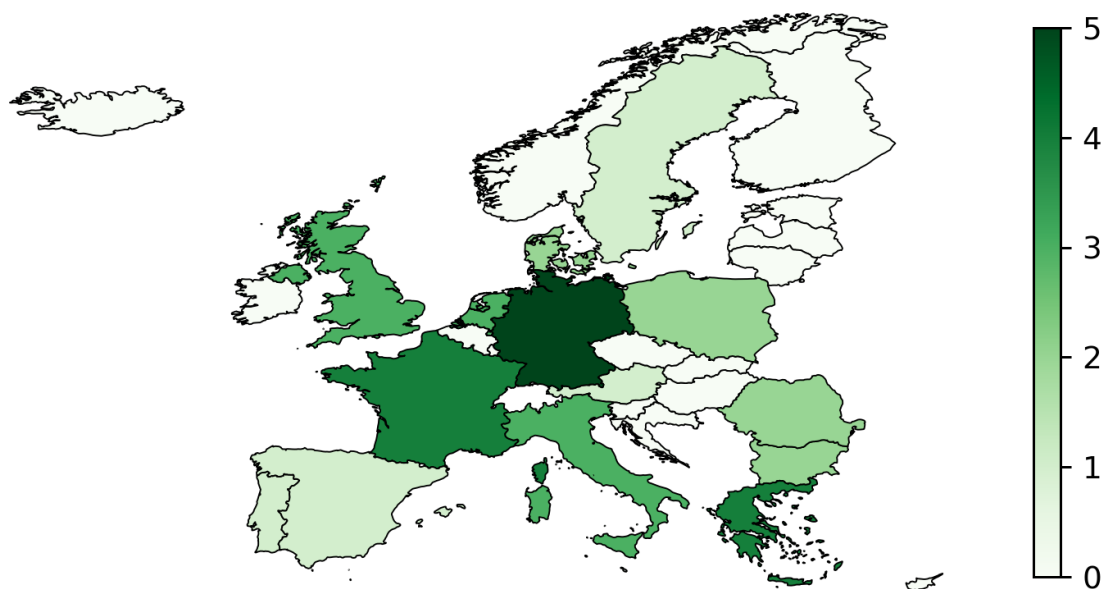
Source: GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed March 27, 2020).

<sup>36</sup> GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed March 27, 2020).

<sup>37</sup> GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed March 27, 2020).

<sup>38</sup> European Commission, “Gross Domestic Product at Market Prices” (accessed May 18, 2020).

**Figure 3:** EU GDPR fines by country in excess of €100,000 (\$108,482) each, May 2018 – March 2020



Source: GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed March 26, 2020).

Industry experts largely predicted that GDPR would herald a period of substantial regulatory oversight coupled with very large fines above €1 million (\$1.1 million).<sup>39</sup> In the first 21 months after GDPR implementation, 11 fines were issued in excess of €1 million (\$1.1 million), which accounted for nearly 10 percent of all fines issued in the EU.<sup>40</sup> Of these fines, 3 were issued by the Italian Data Protection Authority, 2 by the UK ICO, 2 by German DPAs, 1 by France’s CNIL, 1 by Bulgaria’s Personal Data Protection Commission, 1 by the Swedish Data Protection Authority, and 1 by the Austrian Data Protection Authority. Four of these fines were issued as a result of data breaches, which appears to show a willingness by EU DPAs to issue weightier fines for data breach violations under Articles 32 and 33 than for violations under other GDPR articles. Additionally, 3 of the 11 fines were issued against U.S. firms (Marriott and Google, which was fined twice by France and Sweden), while the remaining fines were issued against European firms or government agencies (table 3).

<sup>39</sup> Law.com, “Instant Insights/GDPR: 1 Year Later,” May 16, 2019.

<sup>40</sup> This paper investigates fines that are only €10,000 (\$10,848) or larger issued by EU DPAs.

**Table 3:** List of GDPR fines in excess of €1 million (\$1,087,550), May 2018 – March 2020

Country	Month, Year	Firm fined	Industry	GDPR article violation	Fine million € or £ (million \$)
Austria	October 2019	Austria Post	Newspaper	5	€18 (\$19.6)
Bulgaria	August 2019	National Revenue Agency	Government	32	€2.6 (\$2.8)
France	January 2019	Google	Information services	6	€50 (\$54.4)
Germany	October 2019	Deutsche Wohnen	Property services	5, 25	€14.5 (\$15.8)
Germany	December 2019	1&1 Telecom GmbH	Telecom services	32	€3.6 (\$3.9)
Italy	December 2019	Eni Gas e Luce	Energy services	5, 6, 17, 21	€8.5 (\$9.2)
Italy	December 2019	Eni Gas e Luce	Energy services	5, 6	€3 (\$3.3)
Italy	January 2020	TIM	Telecom services	5, 6, 17, 21	€27.8 (\$30.2)
Sweden	March 2020	Google	Internet services	5, 6, 17	€7 (\$7.6)
United Kingdom	July 2019	Marriott	Hotel services	33	£99 (\$122.4)
United Kingdom	July 2019	British Airways	Transportation services	32	(£183) (\$226)

Source: GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed September 23, 2019).

## United Kingdom

Enforcement action by the UK ICO suggests that the UK DPA has been the most active of the DPAs in issuing heavy fines against firms that violate GDPR, especially with respect to breach notifications.<sup>41</sup> The two most recent examples have been the large fines against British Airways (£183 million fine, \$227 million) and Marriott (£99 million fine, \$123 million) for data breach notification violations.<sup>42</sup> The UK ICO's fine against Marriott was issued in July 2019, after Marriott reported in November 2018 that its computer systems had been breached. The original breach, which had occurred in November 2014 (before GDPR was implemented) after Marriott acquired Starwood, ultimately compromised the passwords and credit card records of 30 million EU residents. The UK ICO's fine against Marriott represented approximately 3 percent of its worldwide annual revenue, which is close to the maximum penalty allowed by GDPR. In the same month, the UK ICO issued another large fine against British Airways for a data breach incident that occurred in June 2018.

<sup>41</sup> TechExpert, "Record-Setting Fines in 2019," September 3, 2019.

<sup>42</sup> TechExpert, "Record-Setting Fines in 2019," September 3, 2019.

Also, in July 2019, those responsible for the data breach redirected customers to a fraudulent website, which ultimately compromised half a million customers' data including their login information, payment card, name, address, and travel booking information.<sup>43</sup> The British Airways fine represented 1.5 percent of its total worldwide revenue.<sup>44</sup> Both British Airways and Marriott have stated that they plan to appeal their respective GDPR fines.

The UK ICO publicly justified issuing such large fines by stating that organizations must be “accountable for the personal data they hold” and that this responsibility includes “carrying out proper due diligence.” The UK ICO also said that organizations have a legal duty to ensure the security of personal data, and “if that doesn’t happen, we will not hesitate to take strong action when necessary to protect the rights of the public.” Before GDPR was implemented, the UK ICO had issued a €500,000 (\$540,000) fine against Cambridge Analytica, which was the maximum fine under the EU Directive.<sup>45</sup> An analysis of GPDR fines issued indicates that the UK ICO has been more proactive than other DPAs in making full use of GDPR’s higher ceiling when determining fines.<sup>46</sup> These industry experts claim UK ICO’s fines likely “set a precedent and serve as a warning to other companies currently under investigation for GDPR violations,” especially U.S.-based companies such as Google and Facebook.<sup>47</sup>

The United Kingdom’s departure from the European Union has led to some discussions of potential changes to GDPR in the UK. UK government officials have mentioned “data sovereignty” when the country transitions out of the EU (Brexit). Nonetheless, the UK government has directly transposed GDPR into national law.<sup>48</sup> As a result, government officials and industry analysts speculated that the legal and regulatory framework under which the UK DPA currently operates is not expected to change post-Brexit. However, after it officially leaves the EU, the UK most likely will no longer have a position in EU-wide GDPR institutions such as the European Data Protection Board. Further, it may or may not receive an adequacy determination<sup>49</sup> from the European Commission regarding whether UK GDPR regulations accord with those of EU GDPR.<sup>50</sup> Without an adequacy determination, the UK may not be able to send, receive, or share

---

<sup>43</sup> Sweny, “GDPR Fines, Where Will BA and Marriott’s 300 Million Fine Go?” July 10, 2019.

<sup>44</sup> Satariano, “After a Data Breach, British Airways Faces a Record Fine,” July 8, 2019; Sweny, “GDPR Fines, Where Will BA and Marriott’s 300 Million Fine Go?” July 10, 2019.

<sup>45</sup> TechExpert, “Record-Setting Fines in 2019,” September 3, 2019.

<sup>46</sup> TechExpert, “Record-Setting Fines in 2019,” September 3, 2019.

<sup>47</sup> TechExpert, “Record-Setting Fines in 2019,” September 3, 2019.

<sup>48</sup> GDPR is incorporated in UK under the EU Withdrawal Agreement, as well as the Data Protection Act 2018. IT Pro, “GDPR and Brexit: How Will One Affect the Other?” May 24, 2019.

<sup>49</sup> An “adequacy determination” is when the European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679, whether a country outside the EU offers an adequate level of data protection. Generally, the adoption of an adequacy decision involves a proposal from the European Commission, an opinion of the European Data Protection Board, an approval from representatives of EU countries, and the adoption of the decision by the European Commission. European Commission, “Adequacy Decisions,” [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en) (accessed March 26, 2020).

<sup>50</sup> DP Network, “Brexit, GDPR, and Data Protection: What Happens if the UK Becomes a Third Country?” (accessed October 7, 2019).

personal data with firms located in the European Union, with implications for a variety of sectors (including travel, banking, insurance, as well as numerous multinational firms).

## France

France's data protection authority, CNIL, mainly focused its attention on targeted advertising, rather than on breach notifications in its initial enforcement activity against firms.<sup>51</sup> In 2018, CNIL issued four initial decisions against French ad-tech companies that provided targeted advertising and marketing services to retailers.<sup>52</sup> CNIL publicly stated that valid consent had not been obtained before collecting data from mobile app users that firms used in processing their geographical data for advertising purposes.<sup>53</sup> In January 2019, CNIL issued its first fine, a €50 million (\$54 million) judgment against Google, for failing to ensure that user data was processed legally for personalized advertisements.<sup>54</sup> This fine represented CNIL's largest fine to date.<sup>55</sup> CNIL argued that France has the authority to impose the fines because the complaints originated in France and the affected parties resided in France.<sup>56</sup> CNIL's early fines collectively imply that CNIL places particular importance on GDPR's principles around transparency and consent, especially in the context of targeted advertisements.<sup>57</sup> Through its initial fines, CNIL has likely signaled to firms that behavioral advertising, and profiling and processing by third parties, will not be tolerated.<sup>58</sup>

CNIL's recent action against Sergic, a French-based real estate company, indicates that France likely considers Article 32 of GDPR, which relates to preserving the security of personal data of users, to be an important data privacy concern.<sup>59</sup> In May 2019, CNIL's second GDPR-related fine was imposed against Sergic because users could access internal documents from other individuals on the site by simply modifying a URL. The documents contained individuals' identity cards, tax notices, account statements, and other information. This vulnerability was discovered by Sergic in March 2018 (before GDPR implementation), but was not remedied until September 2018.<sup>60</sup> CNIL

---

<sup>51</sup> CNIL, "Presentation of the 2018 Activity Report and 2019 Issues of the French Data Protection Authority," (accessed September 25, 2019).

<sup>52</sup> CNIL, "Presentation of the 2018 Activity Report and 2019 Issues of the French Data Protection Authority," (accessed September 25, 2019).

<sup>53</sup> O'Donovan, "CNIL vs. Google: 10 lessons from the Largest Data Protection Fine Ever Issued," January 30, 2019.

<sup>54</sup> Practical Law, "Expert Q&A: Lessons from the CNIL's EUR 50 Million GDPR Enforcement Action Against Google," 2019.

<sup>55</sup> Google is currently arguing that CNIL does not have the proper jurisdiction to issue fines and the case should have been handled by the Irish Data Protection Commissioner as Google's lead supervisory authority, rather than the CNIL, because Google's EU headquarters are in Ireland. Hunton Andrews Kurth LLP, "CNIL Fines Google €50 Million for Alleged GDPR Violations," January 23, 2019; Ikeda, "Google to Pay Record €50 Million GDPR Fines as CNIL Draws Lines in the Sand," January 30, 2019.

<sup>56</sup> Ikeda, "Google to Pay Record €50 Million GDPR Fines as CNIL Draws Lines in the Sand," January 30, 2019.

<sup>57</sup> Practical Law, "Expert Q&A: Lessons from the CNIL's EUR 50 Million GDPR Enforcement Action against Google," 2019.

<sup>58</sup> Practical Law, "Expert Q&A: Lessons from the CNIL's EUR 50 Million GDPR Enforcement Action against Google," 2019.

<sup>59</sup> Martin and Shabestari, "New CNIL €400,000 Fine for Data Security Breaches and Non-compliance with Data Retention Period under the GDPR," July 8, 2019.

<sup>60</sup> Morris, "CNIL Targets Poor Data Security for Second GDPR Fine," June 6, 2019.



stated that it issued a €400,000 (\$431,000) fine because Sergic failed to implement a user authentication protocol, and the fine amount reflects the “seriousness of the breach, the sensitivity of the documents and the company’s size.”<sup>61</sup>

Besides targeted advertising and data security measures, CNIL issued a third GDPR fine for violations concerning video surveillance of employees. In June 2019, CNIL fined Uniontrad Company, a French-based translation company, €20,000 (\$22,000) after discovering that the company continuously filmed six of their employees at their workstations without their consent.<sup>62</sup> These employees were never given information about why they were recorded.<sup>63</sup> From 2013 to 2017, CNIL repeatedly requested that Uniontrad Company stop the practice, but found that this practice continued after auditing the company in February 2018.<sup>64</sup> CNIL’s decision was based on the premise that video surveillance of employees went beyond the firm’s stated purpose—ensuring the security of its employees—and was contrary to the data minimization principle under Article 5 of GDPR.<sup>65</sup>

## Italy

Italy’s data protection authority, Garante per la protezione dei dati personali (Garante), was slower than most EU countries to adopt fines against companies after GDPR was implemented, but it started issuing heavier fines in early 2020. In 2017 (before GDPR was implemented), Garante originally found that Rousseau, an internet platform operated by an Italian political party, Movimento 5 Stelle (Five Star Movement), did not implement sufficient security measures after a data breach and did not update privacy information for its users, which would have given more transparency into the data processing activities performed by the firm.<sup>66</sup> Garante also stated that Rousseau needed to update its security measures after this data breach. However, the Italian data protection authority found that Rousseau had not implemented some GDPR-related security measures after the breach.<sup>67</sup> In April 2019, Garante issued its first GDPR fine—€50,000 (\$54,000)—against Rousseau for having inadequate technical and organizational measures to ensure data security under Article 32 of GDPR. In April 2019, Garante fined Rousseau for its failure both to anonymize e-voting data and to regulate access to personal data on its platform. Interestingly, Garante ultimately held the data processor, Rousseau—rather than the data controller, Movimento 5 Stelle—responsible for GDPR violations.<sup>68</sup> This decision by the Italian

---

<sup>61</sup> Morris, “CNIL Targets Poor Data Security for Second GDPR Fine,” June 6, 2019.

<sup>62</sup> Morris, “CNIL Issues Third GDPR Fine,” June 18, 2019.

<sup>63</sup> IAPP, “CNIL Fines Company 20K Euros for Illicit Employee Surveillance,” June 18, 2019.

<sup>64</sup> Morris, “CNIL Issues Third GDPR Fine,” June 18, 2019.

<sup>65</sup> Ivanišević, “CNIL’s Primer on Video Surveillance at Work: Uniontrad Company Decision” (accessed October 2, 2019).

<sup>66</sup> Advisory 21, “Data Processors Beware: Italy Has Issues its First GDPR Fine” (accessed April 3, 2020).

<sup>67</sup> GDPR Enforcement Tracker, <https://www.enforcementtracker.com/> (accessed April 3, 2020).

<sup>68</sup> GDPR Enforcement Tracker, <https://www.enforcementtracker.com/> (accessed April 3, 2020).



DPA was unique because it recognized that liability could be imparted to the data processor without holding the data controller responsible for GDPR violation.<sup>69</sup>

Although Garante was slower initially to adopt fines, it started levying heavier fines in early 2020 for specific violations relating to targeted advertising via telemarketing calls under Article 5 of GDPR. In January 2020, Garante levied two fines totaling €11.5 million (\$12.4 million)<sup>70</sup> against Eni Gas e Luce (Eni), an Italian energy company. The largest fine against the company was for €8.5 million (\$9.2 million) because the company did not have legitimate grounds to process data and continued to make telemarketing calls without the consent of the data subjects.<sup>71</sup> In many instances, these calls were made even though the data subjects had been placed on “do not call” lists. Garante also found that Eni did not have the technical or corrective measures in place that would enable consent to make those calls and for purchasing customer data from telemarketing lists without explicit consent from data subjects.<sup>72</sup>

In February 2020, Garante imposed its third large fine on a telecommunications company, TIM S.p.A. (TIM or Telecom Italia), in the amount of €27.8 million for making promotional calls without a data subject’s consent.<sup>73</sup> Like the Eni case, some of TIM’s data subjects had placed their numbers on “do not call lists.”<sup>74</sup> In addition to the fine, Garante said that that TIM had to take 20 corrective measures within a prescribed time frame.<sup>75</sup> Besides the fines on the above-mentioned companies, from January 2020 to March 2020, Garante also issued smaller fines, varying from €4,000 to €20,000, for insufficient bases for the legal processing of data under Articles 5 and 6 of GDPR.<sup>76</sup>

## Germany

Germany’s enforcement of GDPR has taken a different approach than that of other major EU Western European countries. One difference is structural; as noted in the textbox above, while France and the UK each have a single DPA with sole authority to issue fines, Germany has multiple DPAs—one per region—and each regional DPA has the authority to levy fines on companies. Another difference is the timing of Germany’s fines; while the UK and France issued multi-million euro fines against non-compliant firms in the first few months after GDPR implementation, no

---

<sup>69</sup> DLA Piper. “Italy’s First Fine Issued!” Privacy Matters, May 8, 2019.

<sup>70</sup> Garante issued two separate fines against Eni Gas e Luce, one in the amount €8.5 million and one for €3 million. The latter fine was issued because of infringements resulting from unsolicited electricity and gas contracts under ‘market economy’ conditions. Many persons complained they were aware of the contracts after receiving letters of their contract termination from the previous supplier, and some of these contracts contained false information and forgeries. GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed April 3, 2020).

<sup>71</sup> IAPP, “Italian DPA Issues 11.5 M Euro GDPR Fine,” January 17, 2020; European Data Protection Board, “The Italian Supervisory Authority Fines Eni Gas e Luce EUR 11 Million,” January 17, 2020.

<sup>72</sup> IAPP, “Italian DPA Issues 11.5 M Euro GDPR Fine,” January 17, 2020; European Data Protection Board, “The Italian Supervisory Authority Fines Eni Gas e Luce EUR 11 Million,” January 17, 2020.

<sup>73</sup> IAPP, “Italian DPA Issues 27.8 M Euros for GDPR Violations,” February 3, 2020.

<sup>74</sup> IAPP, “Italian DPA Issues 27.8 M Euros for GDPR Violations,” February 3, 2020

<sup>75</sup> IAPP, “Italian DPA Issues 27.8 M Euros for GDPR Violations,” February 3, 2020

<sup>76</sup> GDPR Enforcement Tracker, <https://www.enforcementtracker.com/> (accessed April 3, 2020).

German fine exceeded 1 million euro until more than a year after GDPR implementation. It is likely that after GDPR implementation, German DPAs saw their initial role as being supportive of companies by acting as advisors on GDPR's regulations.<sup>77</sup> During this period, German DPAs began slowly imposing relatively low fines on companies and issued very few such fines.<sup>78</sup>

More recently, evidence suggests that certain German DPAs—in particular, the DPAs of Hamburg, Bavaria, Berlin, North Rhine-Westphalia, Hesse, and Baden-Württemberg, as well as the German national DPA—have been more active in issuing fines.<sup>79</sup> For example, the highest fine in Baden-Württemberg of €80,000 (\$87,996) was imposed because sensitive health data were available on the internet due to inadequate data protection, and the data authority of Rheinland-Pfalz issued its highest fine (€100,000, \$110,000) for a mix-up of patient records that disclosed sensitive data.<sup>80</sup> Additionally, other German regulatory authorities, notably the Federal Cartel Office, have cited GDPR in their own enforcement measures.<sup>81</sup>

Despite initially limited enforcement action, industry observers have noted that German DPAs have become increasingly willing to take more aggressive enforcement actions recently, with fines totaling more than €600,000 (\$661,000) by May 2019 and more than €15 million by March 2020.<sup>82</sup> Over this period, German DPAs have fined firms for violations of numerous GDPR provisions including inadequate data security measures, sending unauthorized marketing emails, and processing personal data without an established need.<sup>83</sup> Several German DPA fines have mainly focused on online firms; for example, Knuddels, a German social chat platform, was fined in November 2018 for inadequate data storage policies, and Delivery Hero, a multinational online food delivery service based in Germany, was fined in October 2019 by the Berlin DPA for failing to delete inactive accounts.

Other sectors, particularly in banking and housing, have received attention from German DPAs. In late 2018, a local German bank was fined €50,000 (\$54,998) under Article 6 for processing the personal data of all former customers without user consent.<sup>84</sup> In November 2019, the Berlin DPA announced that it had issued Germany's largest GDPR fine: the apartment and property firm Deutsche Wohnen was fined €14.5 million (\$15.6 million) for storing personal data of tenants without an established purpose, and because the data had been accessible for years to the public

---

<sup>77</sup> Tinnefeld and Hanben, "GDPR Enforcement Update: Increasing Fines Expected from German DPAs," February 22, 2019.

<sup>78</sup> Latham & Watkins, "High GDPR Fines: German Data Protection Authority Joins the Club," August 27, 2019.

<sup>79</sup> Tinnefeld and Hanben, "GDPR Enforcement Update: Increasing Fines Expected from German DPAs," February 22, 2019.

<sup>80</sup> Beck and Worm, "Post GDPR Enforcement in Germany—A Sneak Peek" (accessed September 25, 2019); GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed March 30, 2019).

<sup>81</sup> TechCrunch, "German Antitrust Office Limits Facebook Data Gathering," February 7, 2019.

<sup>82</sup> GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed March 30, 2020).

<sup>83</sup> Beck and Worm, "Post GDPR Enforcement in Germany—A Sneak Peek" (accessed September 25, 2019).

<sup>84</sup> GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed November 13, 2019).

(in violation of articles 5 and 25). The Berlin DPA also issued at least 15 specific fines, ranging from €6,000 to €17,000, to Deutsche Wohnen for individual GDPR violations.<sup>85</sup>

Additionally, although the German regional DPAs carry out many of the data protection and enforcement measures in Germany, the national German DPA has also increasingly taken enforcement action against firms. In December 2019, the German Federal Commissioner for Data Protection fined 1&1 Telecom GmbH (a telecommunications firm operating in Germany) €9.6 million (\$10.3 million) for failing to take sufficient measures to ensure information security (article 32). Combined with the Berlin DPA fine of Deutsche Wohnen, these fines have contributed to Germany's emergence as the third-largest issuer of GDPR fines in the EU (after France and Italy).<sup>86</sup>

## Netherlands

Industry experts note that the Netherlands' GDPR enforcement appears to be focused on protecting the security of data relating to the public and health sectors within the country.<sup>87</sup> This was evidenced by the first fine issued, in July 2019, by the Dutch DPA, Autoriteit Persoonsgegevens, which fined Dutch Haga Hospital €460,000 (\$498,000) for having insufficient internal security for their patient records.<sup>88</sup> The lack of adequate security measures violated GDPR's Article 31 because the hospital did not have a two-factor authentication procedure in place to access patient records.<sup>89</sup> In addition to the fine, the Dutch DPA also imposed a cease and desist order and additional fines of €100,000 per week (up to a maximum of €300,000) if the hospital did not comply by October 2019.<sup>90</sup>

The Netherlands' enforcement regime is different from other countries because it released a GDPR fining policy that has four categories of fines, depending on the company size and the specific violation.<sup>91</sup> Although the Dutch DPA does not explicitly publicize how it categorizes GDPR violations, it does share some factors that determine the fine amount, such as how long the infringement took place, the number of data subjects affected, the amount of time the firm took to respond to the violation, and what type of personal data were affected.<sup>92</sup>

---

<sup>85</sup> GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed November 13, 2019).

<sup>86</sup> The United Kingdom, which has issued fines exceeding France, Italy, and Germany, by value, officially exited the EU on January 31, 2020

<sup>87</sup> DLA Piper, "The Netherlands – First GDPR Fine Imposed: EUR 460,000," July 16, 2019.

<sup>88</sup> DLA Piper, "The Netherlands – First GDPR Fine Imposed: EUR 460,000," July 16, 2019.

<sup>89</sup> *Security Magazine*, "First GDPR Data Breach Imposed in the Netherlands," July 18, 2019.

<sup>90</sup> DLA Piper, "The Netherlands – First GDPR Fine Imposed: EUR 460,000," July 16, 2019; *Security Magazine*, "First GDPR Data Breach Imposed in the Netherlands," July 18, 2019.

<sup>91</sup> Maack, "The Netherlands Premieres the First GDPR Fining Policy in the EU," March 2019.

<sup>92</sup> Maack, "The Netherlands Premieres the First GDPR Fining Policy in the EU," March 2019.

## Ireland

Despite its small market size, DPA enforcement in Ireland has attracted significant interest because many major U.S. digital services providers maintain European headquarters there, placing them under the jurisdiction of the Irish Data Protection Commission (DPC) on most issues. The Irish DPC does have several open investigations focused on U.S.-headquartered technology services providers following the implementation of GDPR. Ireland's investigations appear to vary across GDPR provisions, and likely include investigations for data breaches, lawful processing of personal data, and transparency provisions of user services contracts (table 3). Since GDPR entered into force, the DPC has opened investigations against U.S.-headquartered firms Facebook, Google, Apple, Amazon, Twitter, and Verizon. Despite the open investigations, as of March 2020, the Irish DPC has not issued any major fines to U.S. or other foreign firms regarding violations of GDPR.

**Table 3:** Ongoing investigations by the Irish Data Protection Commission (DPC) on prominent U.S. firms, May 2018–August 2019

U.S. firm	Alleged GDPR violation
<b>Facebook</b>	<ul style="list-style-type: none"> <li>• <i>Right of access:</i> whether Facebook's Hive observed obligations to ensure user data are transferrable.</li> <li>• <i>Lawful processing:</i> whether Facebook's terms of service respect the "lawful basis" for processing personal data; Facebook's use of personal data for behavior analysis and targeted advertising.</li> <li>• <i>Data breach:</i> 5 ongoing investigations regarding whether Facebook met breach notification requirements and technical/organizational obligations before and directly following breaches, as well as whether Facebook violated GDPR in keeping user passwords in plain text on internal servers.</li> </ul>
<b>WhatsApp</b>	<ul style="list-style-type: none"> <li>• <i>Lawful processing:</i> whether WhatsApp's terms of service follow lawful basis for processing personal data.</li> <li>• <i>Transparency:</i> whether WhatsApp meets transparency obligations on information provided to users.</li> </ul>
<b>Instagram</b>	<ul style="list-style-type: none"> <li>• <i>Lawful processing:</i> whether Instagram's terms of service follow lawful basis for processing personal data.</li> </ul>
<b>Twitter</b>	<ul style="list-style-type: none"> <li>• <i>Right of access:</i> whether Twitter's ability for users to have equal access to the same links meets GDPR right of access obligations.</li> <li>• <i>Data breach:</i> whether Twitter met technical/organizational obligations to safeguard data following a breach.</li> </ul>
<b>LinkedIn</b>	<ul style="list-style-type: none"> <li>• <i>Lawful processing:</i> LinkedIn's use of personal data for behavior analysis and targeted advertising.</li> </ul>
<b>Apple</b>	<ul style="list-style-type: none"> <li>• <i>Lawful processing:</i> Apple's use of personal data for behavior analysis and targeted advertising.</li> <li>• <i>Transparency:</i> whether Apple meets its transparency obligations with respect to its privacy policy.</li> <li>• <i>Data access:</i> whether Apple meets its data access request obligations under GDPR.</li> </ul>
<b>Google</b>	<ul style="list-style-type: none"> <li>• <i>Lawful processing:</i> Google's use of personal data for behavior analysis and targeted advertising. The investigation will also look at <i>transparency</i> and <i>data minimization</i> obligations under GDPR.</li> </ul>
<b>Quantcast</b>	<ul style="list-style-type: none"> <li>• <i>Lawful processing:</i> Quantcast's use of personal data for behavior analysis and targeted advertising.</li> </ul>
<b>Verizon</b>	<ul style="list-style-type: none"> <li>• <i>Lawful processing:</i> whether Verizon's use of online cookies complied with lawful processing requirements.</li> </ul>

Note: Both WhatsApp and Instagram are owned by Facebook, Inc. LinkedIn is owned by Microsoft.

Source: Irish Data Protection Commission website, <https://www.dataprotection.ie/>; Ireland DPC, "Annual Report: May 25-December 31, 2018," February 2019.

Some EU member states' DPAs have expressed concern that Ireland is allowing major GDPR violations to occur despite its numerous investigations, thereby creating a "regulatory safe zone" within the EU.<sup>93</sup> Ireland has historically attracted a number of technology firms to headquarter their EU operations in the country due to its attractive tax structure, easy access to officials, and ease of securing investment.<sup>94</sup> Data privacy experts and EU regulators have expressed skepticism on Ireland's commitment to privacy principles in GDPR because other EU countries perceive a lack of policing in Ireland on such privacy-related topics as facial-recognition software and sharing data across platforms.<sup>95</sup>

One of the most significant judgments from the Irish DPC did not involve a firm but rather related to an Irish government initiative. In August 2019, the DPC found that Ireland's Department for Employment Affairs and Social Protection had violated several components of GDPR during the issuance of its Public Services Card (PSC). The PSC was designed to serve as an identity verifier in order to access an array of public services. In 2011, the PSC focused exclusively on social welfare payments, but was later extended to travel, passport, and citizenship applications, as well as driving tests and licenses. The social welfare services include maternity/paternity payments, pensions, child benefits, and unemployment. The broad spectrum of services covered by the PSC required the transfer of Irish residents' personal data across several government departments for a variety of purposes. The justification for the DPC's ruling against the PSC was the absence of consent for data use at each stage. The Irish government is currently contesting the DPC's ruling in court.<sup>96</sup>

## Eastern Europe

Eastern European DPAs have implemented fewer fines (and fewer large fines) than their Western European counterparts. Most fines have focused on domestically headquartered firms, small organizations, government agencies, and political parties. Of the 107 fines exceeding €10,000 issued across Europe between May 2018 and March 2020, 26 (23 percent) have originated in Eastern Europe. Of fines exceeding €100,000, 10 of the 35 issued in the same period (29 percent) were imposed by Eastern European DPAs.

Four countries—Bulgaria, Hungary, Poland, and Romania—have imposed the vast majority of both large and very large fines in Eastern Europe. Bulgaria in particular stands out for its fines: in August 2019, it issued two fines for violations of Article 32 of GDPR (regarding the lack of sufficient protective measures that led to a hack of personal data).<sup>97</sup> One fine (€511,000, or \$551,000) was issued against DSK Bank, a major Bulgarian bank, while the other (€2.6 million,

---

<sup>93</sup> Vinocaur, "One Country Blocks the World on Data Privacy," April 25, 2019.

<sup>94</sup> Vinocaur, "One Country Blocks the World on Data Privacy," April 25, 2019.

<sup>95</sup> Vinocaur, "One Country Blocks the World on Data Privacy," April 25, 2019.

<sup>96</sup> Horgan-Jones, "Government Will Not Comply with Findings on Public Services Card," September 17, 2019.

<sup>97</sup> GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed April 9, 2020).



or \$2.8 million) was levied on Bulgaria's National Revenue Agency. Both reflected trends throughout Europe (and particularly Eastern Europe) focusing on enforcement actions against banks and government agencies.<sup>98</sup>

While it appears that Western European DPAs have often investigated and occasionally fined non-domestic firms, most Eastern European enforcement actions appear to have focused on domestic firms. In Romania, for example, domestically headquartered banks, a credit agency, and a hotel were fined for GDPR violations, typically in relation to data breaches or improper protection of customer data.

## Impact of EU Enforcement of U.S. Firms

While the majority of GDPR fines have been issued against European firms, individuals, and government agencies, DPAs across Europe have initiated enforcement actions against U.S. firms for GDPR violations. To date, major GDPR fines have been issued against three U.S. firms.<sup>99</sup> These firms—Google, Marriott, and PricewaterhouseCoopers<sup>100</sup> (PwC)—faced fines ranging from €150,000 (\$165,400) to £99 million (\$123 million). The fines were issued by four different EU member states, citing different types of GDPR violations. Google's €50 million (\$54 million) fine was issued by France for violation of Article 6 regarding consent and transparency, while the €7 million (\$7.6 million) fine it received from Sweden was due to insufficient fulfillment of data subject rights under Articles 5 and 6. Marriott's £99 million fine was issued by the UK as a result of an Article 33 violation, which addresses data breach notification requirements. PwC's €150,000 fine was issued by Greece for violating Article 83, which covers fairness and transparency principles of using employee data for commercial purposes. In some instances, DPAs do not disclose the name of the company being fined, making it difficult to discern whether a U.S., European, or other firm has faced a fine.<sup>101</sup>

Several U.S. companies, such as Google and Marriott, that have been subject to large fines have publicly stated that they intend to appeal their fines. There is no precedent on how the appeals process would work for GDPR violations.<sup>102</sup> In most instances, when a company files an appeal, the execution of the fine is suspended until a final judgment is delivered by a court.<sup>103</sup> Google

---

<sup>98</sup> GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed April 9, 2020).

<sup>99</sup> In addition, one GDPR fine was issued to then-U.S.-owned Avon Cosmetics, though Avon has since been purchased by a Brazilian conglomerate. Abogados, "AEPD Fines Avon with 60,000 Euros," September 10, 2019.

<sup>100</sup> Despite its London headquarters, PwC in 2018 was ranked as one of the largest U.S. firms not publicly listed. *Forbes*, "America's Largest Private Companies" (accessed September 26, 2019).

<sup>101</sup> For example, in August 2019 the Berlin DPA in Germany issued a €200,000 fine against an "online company," the largest fine issued up to that point in Germany. JDSupra, "High GDPR Fines: German Data Protection Authority Joins the Club," August 28, 2019.

<sup>102</sup> Travers Smith LLP, "You've Been Fined: What Should You Do Next?" (accessed April 21, 2020).

<sup>103</sup> Baker McKenzie, "First Fine for Violation of the GDPR in Poland," March 28, 2019.

stated that it is appealing its fine to the French Supreme Administrative Court (Conseil d'État) because its consent process for personalized ads is “as transparent and straightforward as possible, based on regulatory guidance and user experience testing.”<sup>104</sup>

U.S. companies appear to have several different avenues for recourse, although some of these avenues may be limited. One of the last avenues for appeal is the European Court of Justice, which is the avenue for appealing EU decisions, whether they are made by an EU DPA or an EU court.<sup>105</sup> However, judicial review by a court is limited because it can only address the way in which a DPA reached a decision, and not the decision to award a fine or the amount to award as a fine.<sup>106</sup>

Some U.S. firms appeal these fines based on questions of jurisdiction. GDPR has a “one-stop-shop” provision for foreign firms that operate in multiple EU jurisdictions, allowing them to designate a “main establishment” in a certain EU country and be subject to enforcement actions solely through the main establishment’s lead DPA.<sup>107</sup> Under GDPR, a “main establishment” is defined as the location of the firm’s central administration within an EU country and may be determined by certain factors, such as where the company is registered, where its directors reside, or where its business decisions are made.<sup>108</sup> However, the presumption of a “main establishment” can be overturned if data processing takes place in another EU member state.<sup>109</sup>

The case of Google illustrates this phenomenon. The U.S. firm’s headquarters are in Ireland, but Google had not yet designated Ireland as its main establishment.<sup>110</sup> France’s CNIL found that it had the authority to issue a fine against Google because Google’s subsidiary, Google Ireland, did not have the “decision-making power of processing operations” of its Android operating system and Google accounts, and therefore Google (the parent company) lacked a main establishment in the EU.<sup>111</sup> The CNIL acknowledged that since Google did not have a main establishment, the U.S. firm might also be subject to additional fines by other DPAs within Europe (as noted earlier, Sweden subsequently fined Google for other GDPR violations in March 2020).<sup>112</sup> Industry sources in the technology sector stated that the CNIL had an interest in acting quickly to fine Google because Google was making preparations to move its main establishment to Ireland after GDPR was implemented in May 2018.

---

<sup>104</sup> Cerelus, “Google to Appeal 50 Million Euro Fine,” January 23, 2019.

<sup>105</sup> Travers Smith LLP, “You’ve Been Fined: What Should You Do Next?” (accessed April 21, 2020).

<sup>106</sup> Travers Smith LLP, “You’ve Been Fined: What Should You Do Next?” (accessed April 21, 2020).

<sup>107</sup> Porzio Life Sciences, “French Data Protection Authority Levies 50 Million Against Google,” February 7, 2019.

<sup>108</sup> Nathan Trust, “Understanding Main Establishment under the GDPR for non-EU Companies,” (accessed June 1, 2020).

<sup>109</sup> Taylor Wessing, “Territorial Scope and Establishment under the GDPR,” April 2016.

<sup>110</sup> Porzio Life Sciences, “French Data Protection Authority Levies 50 Million Against Google,” February 7, 2019.

<sup>111</sup> Porzio Life Sciences, “French Data Protection Authority Levies 50 Million Against Google,” February 7, 2019.

<sup>112</sup> Porzio Life Sciences, “French Data Protection Authority Levies 50 Million Against Google,” February 7, 2019.

Some industry experts speculate that these types of actions will open up a “new era of privacy litigation between companies and [DPAs].”<sup>113</sup> The example of actions against Google caused some companies to analyze more quickly which of their EU establishments would best qualify as a main establishment (based on a firm’s decision-making powers and financial resources) and to designate a lead DPA to handle their GDPR matters.<sup>114</sup> Without companies designating a “main establishment” in a timely manner, they risk more investigations and fines across multiple DPAs in Europe, and this risk continues to cause considerable uncertainty for firms operating in multiple EU member states.<sup>115</sup>

In several instances, once-lawful activities carried out by firms and governments have subsequently been ruled to be unlawful. This has led firms and governments to grapple with how to effectively advance their business or government priorities without running afoul of GDPR.<sup>116</sup> The GDPR enforcement process by DPAs has led to the clarification of terms, the penalizing of formerly legal practices, and increased scrutiny of industries that appear to have been unprepared to incorporate the privacy and data protection standards of GDPR into corporate operations.<sup>117</sup>

Many U.S. firms have changed or clarified their user agreements to ask for explicit consent, as stated in GDPR.<sup>118</sup> Google stated that it was “concerned about the impact of the [French] ruling on publishers, original content creators and tech companies in Europe and beyond.”<sup>119</sup> Industry experts view the result of Google’s appeal as a way for U.S. firms to get clearer guidance on how GDPR will be applied in the future, including detailed definitions on what constitutes transparency and consent with respect to data collection.<sup>120</sup> However, if Google’s appeal is ultimately rejected, industry experts surmise that Google would have to change its business practice regarding how it presents its consent forms to users in order to be in line with the CNIL’s requirements, which would eventually affect many U.S. companies doing business in Europe.<sup>121</sup>

---

<sup>113</sup> De Brauw, Blackstone, and Westbrook, “First Big GDPR Fine for Google: Implications for Multinationals,” January 31, 2019.

<sup>114</sup> De Brauw, Blackstone, and Westbrook, “First Big GDPR Fine for Google: Implications for Multinationals,” January 31, 2019.

<sup>115</sup> De Brauw, Blackstone, and Westbrook, “First Big GDPR Fine for Google: Implications for Multinationals,” January 31, 2019.

<sup>116</sup> Akin & Gump, “A Year of GDPR: Five Recommendations to Help Limit Regulatory Scrutiny,” May 30, 2019.

<sup>117</sup> Akin & Gump, “A Year of GDPR: Five Recommendations to Help Limit Regulatory Scrutiny,” May 30, 2019.

<sup>118</sup> Fefer and Archick, “EU Data Protection Rules and U.S. Implications,” CRS, April 14, 2020.

<sup>119</sup> Porter, “Google fined €50 million for GDPR violation in France,” The Verge, January 21, 2019.

<sup>120</sup> Davis, “Why Google’s Fine and Appeal are Good for Enterprise IT,” January 28, 2019; Murtaza and Salman, “GDPR Fine Imposed Upon Google: An Analysis,” (accessed June 1, 2020).

<sup>121</sup> Murtaza and Salman, “GDPR Fine Imposed Upon Google: An Analysis,” (accessed June 1, 2020).



## Conclusion

After nearly two years of enforcement actions by EU member state DPAs, several preliminary trends have begun to emerge. First, Western European countries appear to be taking a more active approach relative to their Eastern European counterparts in targeting multinational companies by levying very large fines (those in excess of €1 million, or \$1.1 million). Industry experts speculate that this trend of imposing substantial fines will continue, and some EU DPAs, such as the UK ICO, have now stated that the public should expect more regulatory actions against firms that fail to secure and protect user data. These initial public statements from EU authorities have corresponded with the steady increase in fines.

Second, divergences in GDPR interpretations and fines by EU member DPAs appear to be reflective of inconsistent enforcement of EU data protection laws across Europe.<sup>122</sup> Data privacy experts claim that the uneven enforcement and fine levels for GDPR violations throughout the EU have led to uncertainty and changes in business practices among U.S. firms when doing business in Europe.<sup>123</sup> Some U.S. firms have adjusted to this divergence by becoming increasingly informed on GDPR guidance that is produced by each member DPA, as well as the EU Data Protection Board.<sup>124</sup> In some instances, though, uncertainty may arise when guidance from DPAs conflicts with that of the EU Data Protection Board.<sup>125</sup>

Given the issues of increasing scrutiny by EU countries of EU, U.S. and multinational firms, as well as the divergences across EU member states, questions regarding the EU GDPR appeals process are likely to become increasingly important. Because GDPR implementation is still fairly recent, one of the major areas yet to be explored in the enforcement process is exactly how this appeals process will work in practical terms for firms trying to navigate the EU's data protection framework.

---

<sup>122</sup> Gabel, "Chapter 17: Issues Subject to National Law: Unlocking the EU General Data Protection Regulation," April 5, 2019.

<sup>123</sup> Satariano, "Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates," April 28, 2020.

<sup>124</sup> Gabel, "Chapter 17: Issues Subject to National Law: Unlocking the EU General Data Protection Regulation," April 5, 2019.

<sup>125</sup> Gabel, "Chapter 17: Issues Subject to National Law: Unlocking the EU General Data Protection Regulation," April 5, 2019.

## Bibliography

- Abogados, Abril. “AEPD Fines Avon with 60,000 Euros for Including the Data of a Customer in a Debtors’ List.” *Abril Informa* (blog), September 10, 2019. <https://www.abrilabogados.us/aepd-fines-avon-with-60000-euros-for-including-the-data-of-a-customer-in-a-debtors-list/>.
- Advisory 21* (blog) (Malta). “Data Processors Beware: Italy Has Issued Its First GDPR Fine.” <https://www.advisory21.com/mt/data-processors-beware-italy-has-issued-its-first-gdpr-fine/> (accessed April 3, 2020).
- Akin & Gump. “A Year of GDPR: Five Recommendations to Help Limit Regulatory Scrutiny.” Cybersecurity, Privacy, and Data Protection Alert, May 30, 2019. <https://www.akingump.com/en/news-insights/a-year-of-gdpr-five-recommendations-to-help-limit-regulatory.html>.
- Baker McKenzie. “First Fine for Violation of the GDPR in Poland.” March 28, 2019. <https://www.bakermckenzie.com/en/insight/publications/2019/03/first-fine-for-violation-of-the-gdpr>.
- Baxter, Michael. “GDPR Court Decisions Still Only a Trickle: There May Be a Deluge Yet.” PrivSec Report news article, August 7, 2018. <https://gdpr.report/news/2018/08/07/gdpr-court-decisions-still-only-a-trickle-there-might-be-a-deluge-yet/>.
- Beck, Benjamin, and Ulrich Worm. “Post GDPR Enforcement in Germany—A Sneak Peek.” *Mayer Brown*, 19, Issue 5. <https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2019/04/privacy-and-data-protection--post-gdpr-enforcement-in-germany--a-sneak-peek--benjamin-beck--ulrich-worm-mayer-brown-volume-19-issue-5.pdf>.
- Buckbee, Michael. “GDPR Protection Supervisory Authority Listing.” Varonis, April 8, 2019. <https://www.varonis.com/blog/gdpr-data-protection-authority-supervisory-listing/>.
- Cerelus, Laurens. “Google to Appeal 50 Million Euro Fine.” Politico. January 23, 2019. <https://www.politico.eu/article/google-appeals-e50-million-gdpr-fine/>.
- Cherepanova, Vera. “GDPR Enforcement Report (May 2019).” *FCPA Blog*, May 14, 2019. <https://www.fcablog.com/blog/2019/5/14/gdpr-enforcement-report-may-2019.html>.
- Congressional Research Service (CRS). *Trade Adjustment Assistance (TAA) and Its Role in U.S. Trade Policy*, by J.F. Hornbeck. CRS Report R41922, August 5, 2013. <http://www.fas.org/sgp/crs/misc/R41922.pdf>.

## EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

- Commission Nationale de L'Informatique et des Libertés (CNIL). “Presentation of the 2018 Activity Report and 2019 Issues of the French Data Protection Authority.” April 15, 2019. <https://www.cnil.fr/en/presentation-2018-activity-report-and-2019-issues-french-data-protection-authority> (accessed September 25, 2019).
- Davis, Jessica. “Why Google’s Fine and Appeal Are Good for Enterprise IT.” Information Week. January 28, 2019. <https://www.informationweek.com/strategic-cio/security-and-risk-strategy/why-googles-gdpr-fine-and-appeal-are-good-for-enterprise-it/a/d-id/1333732>.
- De Brauw, Blackstone, and Westbroek, “First Big GDPR Fine for Google: Implications for Multinationals.” January 31, 2019. <https://www.debrauw.com/alert/first-big-gdpr-fine-for-google-implications-for-multinationals/>.
- DLA Piper (blog). “Italy’s First Fine Issued!” Privacy Matters, May 8, 2019. <https://blogs.dlapiper.com/privacymatters/italy-first-gdpr-fine-issued/>.
- DLA Piper (blog). “The Netherlands—First GDPR Fine Imposed: EUR 460,000.” Privacy Matters, July 16, 2019. <https://blogs.dlapiper.com/privacymatters/the-netherlands-first-gdpr-imposed-eur-460000/>.
- DP Network. “Brexit, GDPR, and Data Protection: What Happens If the UK Becomes a Third Country?” n.d. <https://www.dpnetwork.org.uk/brexit-gdpr-data-protection-uk/> (accessed October 7, 2019).
- Electronic Privacy Information Center (EPIC). “Austrian Supreme Court: GDPR Lawsuits Can Be Filed Throughout EU.” June 13, 2019. <https://epic.org/2019/06/austrian-supreme-court-gdpr-la.html>.
- European Commission (EC). “Adequacy Decisions.” [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en) (accessed March 26, 2020).
- European Commission (EC). “Communication from the Commission to the European Parliament and the Council: Data Protection Rules as a Trust-Enabler in the EU and Beyond—Taking Stock.” July 24, 2019. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2019:374:FIN>.
- European Commission (EC). “Data Protection in the EU.” [https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en) (accessed September 26, 2019).
- European Commission (EC). “Gross Domestic Product at Market Prices.” n.d. <https://ec.europa.eu/eurostat/tgm/refreshTableAction.do?tab=table&plugin=1&init=1&pcode=tec00001&language=en> (accessed May 18, 2020).

EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

European Commission (EC). “What Is the European Data Protection Board (EDPB)?”

[https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en) (accessed September 25, 2019).

European Data Protection Board, “The Italian Supervisory Authority Fines Eni Gas e Luce EUR 11 Million.” January 17, 2020. [https://edpb.europa.eu/news/national-news/2020/italian-supervisory-authority-fines-eni-gas-e-luce-eur-115-million-account\\_en](https://edpb.europa.eu/news/national-news/2020/italian-supervisory-authority-fines-eni-gas-e-luce-eur-115-million-account_en).

Fefer, Rachel and Kristin Archick. “EU Data Protection Rules and U.S. Implications”

Congressional Research Service (CRS). April 14, 2020.

<https://fas.org/sgp/crs/row/IF10896.pdf>.

*Forbes*. “America’s Largest Private Companies.” n.d.

<https://www.forbes.com/largest-private-companies/list/> (accessed September 26, 2019).

Fox Rothschild. “Expert Q&A: Lessons from the CNIL’s EUR 50 Million GDPR Enforcement Action Against Google.” 2019.

<https://www.foxrothschild.com/content/uploads/2019/04/Expert-QAndA-Lessons-from-CNILs-EUR50-Million-GDPR-Enforcement-Action-Against-Google-W-018-6401-1.pdf>.

Future of Privacy Forum. “Case-Law (CJEU, ECHR, national courts).” n.d. <https://fpf.org/case-law-cjeu-echr-national-courts/> (accessed September 26, 2019).

Gabel, Detlav. “Chapter 14: Data Protection Authorities—Unlocking the EU General Data Protection Regulation.” White & Case, April 5, 2019.

<https://www.whitecase.com/publications/article/chapter-14-data-protection-authorities-unlocking-eu-general-data-protection>.

Gabel, Detlav. “Chapter 17: Issues Subject to National Law: Unlocking the EU General Data Protection Regulation.” White & Case, April 5, 2019.

<https://www.whitecase.com/publications/article/chapter-17-issues-subject-national-law-unlocking-eu-general-data-protection>.

General Data Protection Regulation (GDPR EU). “Fines and Penalties.” n.d.

<https://www.gdpreu.org/compliance/fines-and-penalties/> (accessed September 26, 2019).

General Data Protection Regulation (GDPR). Article 77. “Right To Lodge a Complaint With A Supervisory Authority.” <https://gdpr-info.eu/art-77-gdpr/> (accessed September 25, 2019).

General Data Protection Regulation (GDPR) Enforcement Tracker.

<http://www.enforcementtracker.com/> (accessed September 20, 2019).

Government of France. Commission Nationale de l'Informatique et des Libertés (CNIL) [French Data Protection Authority]. "Presentation of the 2018 Activity Report and 2019 Issues of the French Data Protection Authority." <https://www.cnil.fr/en/presentation-2018-activity-report-and-2019-issues-french-data-protection-authority> (accessed September 25, 2019).

Government of Ireland. Irish Data Protection Commission. "DPC Statement on Matters Pertaining to the Public Services Card." August 16, 2019. <https://www.dataprotection.ie/en/dpc-statement-matters-pertaining-public-services-card-0>.

Government of the United Kingdom (UK). Information Commissioner's Office. Twitter, September 12, 2019. <https://twitter.com/ICOnews/status/1172085036012711936/photo/1>.

Holland, Patrick. "Hands On with Pixel 4 and 4 XL: Google's New Phones Only Have Minor Differences." CNET, October 20, 2019. <https://www.cnet.com/news/pixel-4-4-xl-hands-on-google-ditches-fingerprint-scanner-face-unlock/>.

Horgan-Jones, Jack. "Government Will Not Comply with Findings on Public Services Card." *Irish Times*, September 17, 2019. <https://www.irishtimes.com/news/ireland/irish-news/government-will-not-comply-with-findings-on-public-services-card-1.4021397>.

Hunton Andrews Kurth. "CNIL Fines Google €50 Million for Alleged GDPR Violations." Hunton Privacy Blog, January 23, 2019. <https://www.huntonprivacyblog.com/2019/01/23/cnil-fines-google-e50-million-for-alleged-gdpr-violations/>.

Ikeda, Scott. "Google to Pay Record €50 Million GDPR Fines as CNIL Draws Lines in the Sand." *CPO Magazine*, January 30, 2019. <https://www.cpomagazine.com/data-protection/google-to-pay-record-e50-million-gdpr-fines-as-cnil-draws-lines-in-the-sand/>.

International Association of Privacy Professionals (IAPP). "CJEU Releases Judgement on Fashion ID Case." July 29, 2019. <https://iapp.org/news/a/cjeu-rules-websites-responsible-for-data-processing-via-facebook-like-button/>.

International Association of Privacy Professionals (IAPP). "CNIL Fines Company 20K Euros for Illicit Employee Surveillance." June 18, 2019. <https://iapp.org/news/a/cnil-fines-company-20k-euros-for-illicit-employee-surveillance/>.

International Association of Privacy Professionals (IAPP). "Italian DPA Issues 11.5 M Euro GDPR Fine." January 17, 2020. <https://iapp.org/news/a/italian-dpa-issues-11-5m-euro-gdpr-fine/>.

EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

International Association of Privacy Professionals (IAPP). “Italian DPA Issues 27.8 M Euros for GDPR Violations.” February 3, 2020. <https://iapp.org/news/a/italian-dpa-fines-spa-27-8m-euros-for-gdpr-violations/>.

Irish Data Protection Commission. “The Data Protection Commission.” N.d. (accessed June 1, 2020). <https://www.dataprotection.ie/>.

Ireland Data Protection Commission. “Annual Report: May 25-December 31, 2018,” February 2019. <https://www.dataprotection.ie/sites/default/files/uploads/2020-02/DPC%20Annual%20Report%202019.pdf>.

IT Pro (UK). “GDPR and Brexit: How Will One Affect the Other?” May 24, 2019. <https://www.itpro.co.uk/policy-legislation/31772/gdpr-and-brexit-how-will-one-affect-the-other>.

Ivanišević, Bogdan. “CNIL’s Primer on Video Surveillance at Work: Uniontrad Company Decision.” *BDK Advokati* (blog), July 1, 2019. <https://bdkadvokati.com/cnils-primer-on-video-surveillance-at-work-uniontrad-company-decision/>.

JDSupra. “High GDPR Fines: German Data Protection Authority Joins the Club.” August 28, 2019. <https://www.jdsupra.com/legalnews/high-gdpr-fines-german-data-protection-61577/>.

Latham & Watkins. “High GDPR Fines: German Data Protection Authority Joins the Club.” Global Privacy Blog, August 27, 2019. <https://www.globalprivacyblog.com/gdpr/high-gdpr-fines-german-data-protection-authority-joins-the-club/>.

Law.com. “Instant Insights/GDPR: 1 Year Later.” May 16, 2019. <https://www.law.com/corpcounsel/2019/05/16/larger-gdpr-fines-are-on-the-way-privacy-experts-say/?slreturn=20190826124221>.

Lord, Nate. “What Is the Data Protective Directive? Predecessor to the GDPR.” Digital Guardian, September 12, 2018. <https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr>.

Maack, Mar Masson. “The Netherlands Premieres the First GDPR Fining Policy in the EU.” The Next Web, March 2019. <https://thenextweb.com/eu/2019/03/14/the-netherlands-premieres-the-first-gdpr-fining-policy-in-the-eu/>.

EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

Martin, Nadège and Nilofar Moïni Shabestari. “New CNIL €400,000 Fine for Data Security Breaches and Non-compliance with Data Retention Period under the GDPR.” Data Protection Report. July 8, 2019. <https://www.dataprotectionreport.com/2019/07/new-cnil-e400000-fine-for-data-security-breaches-and-non-compliance-with-data-retention-period-under-the-gdpr/>.

Mondschein, Christopher, Cosimo Monda, Pieter Kubben, Michel Dumontier, and Andre Dekker. “Chapter 5, GDPR in a Research Context.” December 22, 2018. <https://pubmed.ncbi.nlm.nih.gov/31314241/>.

Morris, Lauren. “CNIL Issues Third GDPR Fine.” *Global Data Review*, June 18, 2019. <https://globaldatareview.com/article/1194157/cnil-issues-third-gdpr-fine>.

Morris, Lauren. “CNIL Targets Poor Data Security for Second GDPR Fine.” *Global Data Review*, June 6, 2019. <https://globaldatareview.com/article/1193771/cnil-targets-poor-data-security-for-second-gdpr-fine>.

Murtaza, Ghulam, and Salman, Saim. “GDPR Fine Imposed Upon Google: An Analysis.” Brown University, n.d. <http://cs.brown.edu/courses/csci2390/assign/gdpr/ssalman1-gmurtaza-google.pdf> (accessed October 31, 2019).

Nathan Trust. “Understanding Main Establishment under the GDPR for non-EU Companies.” n.d. <https://www.nathantrust.com/insights/understanding-main-establishment-under-the-gdpr-for-non-eu-companies> (accessed June 1, 2020).

O’Donovan, Alice. “CNIL vs. Google: 10 Lessons from the Largest Data Protection Fine Ever Issued.” McGuireWoods, January 30, 2019. <https://www.passwordprotectedlaw.com/2019/01/cnil-vs-google-largest-fine/>.

Organisation for Economic Cooperation and Development (OECD). “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.” 2013. <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm> (accessed September 25, 2019).

Organisation for Economic Cooperation and Development (OECD). “Thirty Years After: the OECD Privacy Guidelines.” 2011. <http://www.oecd.org/sti/ieconomy/49710223.pdf>.

Porter, Jon. “Google fined €50 million for GDPR violation in France.” The Verge, January 21, 2019. <https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil>.

Porzio Life Sciences. “French Data Protection Authority Levies €50 Million Fine Against Google in First Significant GDPR Enforcement Action.” February 7, 2019.

EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

<http://porziolifesciences.com/publications/french-data-protection-authority-levies-50-million-fine-against-google-in-first-significant-gdpr-enforcement-action/>.

Practical Law, “Expert Q&A: Lessons from the CNIL’s EUR 50 Million GDPR Enforcement Action Against Google,” 2019.

<https://www.foxrothschild.com/content/uploads/2019/04/Expert-QAndA-Lessons-from-CNILs-EUR50-Million-GDPR-Enforcement-Action-Against-Google-W-018-6401-1.pdf>.

Runte, Christian, and Schneider, Florian. “Data Law Navigator.” July 11, 2019.

<https://cms.law/en/INT/Publication/Data-Law-Navigator/Germany>.

Satariano, Adam. “After a Data Breach, British Airways Faces a Record Fine.” *New York Times*, July 8, 2019. <https://www.nytimes.com/2019/07/08/business/british-airways-data-breach-fine.html>.

Satariano, Adam. “Europe’s Privacy Law Hasn’t Shown Its Teeth, Frustrating Advocates.” April 27, 2020. <https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html>.

Schmidt, Oliver. “Germany’s First Fine under GDPR Offers Enforcement Insights.” International Association of Privacy Professionals (IAPP), November 27, 2018.

<https://iapp.org/news/a/germanys-first-fine-under-the-gdpr-offers-enforcement-insights/>.

Schultz, Ray. “German Authorities Issue 41 Fines: Report.” International Association of Privacy Professionals (IAPP), February 25, 2019. <https://iapp.org/news/a/german-dpas-issued-41-fines-for-gdpr-violations/>.

Schulze, Elizabeth. “Uber Fined Nearly \$1.2 million by British and Dutch Authorities for 2016 Data Breach.” CNBC, November 27, 2018. <https://www.cnn.com/2018/11/27/uber-fined-more-than-1-million-dollars-by-uk-and-dutch-authorities.html>.

*Security Magazine*. “First GDPR Data Breach Imposed in the Netherlands.” July 18, 2019.

<https://www.securitymagazine.com/articles/90559-first-gdpr-data-breach-fine-imposed-in-the-netherlands>.

Sweney, Mark. “GDPR Fines, Where Will BA and Marriott’s 300 Million Fine Go?” *Guardian*, July 10, 2019. <https://www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog>.

Taylor Wessing. “Territorial Scope and Establishment under the GDPR.” April 2016.

<https://globaldatahub.taylorwessing.com/article/territorial-scope-and-establishment-under-the-gdpr>.



TechCrunch. "German Antitrust Office Limits Facebook Data Gathering." February 7, 2019. <https://techcrunch.com/2019/02/07/german-antitrust-office-limits-facebooks-data-gathering/>.

Techiexpert. "Record-Setting Fines in 2019." September 3, 2019. <https://www.techiexpert.com/record-setting-gdpr-fines-in-2019/>.

Tinnefeld, Christian, and Henrik Hanben. "GDPR Enforcement Update: Increasing Fines Expected from German DPAs." Hogan Lovells, February 22, 2019. <https://www.hldataprotection.com/2019/02/articles/international-eu-privacy/gdpr-enforcement-update-increasing-fines-expected-from-german-dpas/>.

Travers Smith LLP, "You've Been Fined: What Should You Do Next?" n.d. <https://www.lexology.com/library/detail.aspx?g=a62e33e8-7111-4d55-bf3e-74ecf2c9db0a> (accessed October 31, 2019).

Vinocaur, Nicholas. "One Country Blocks the World on Data Privacy." *Politico*, April 25, 2019. <https://www.politico.eu/interactive/ireland-blocks-the-world-on-data-privacy/>.

Waterson, Jim, "UK Fines Facebook £500,000 for Failing to Protect User Data." *Guardian*. October 25, 2018. <https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica>.

## Appendix A

**Table A.1:** Fines in excess of €10,000 (fines in excess of €100,000 are italicized), country of origin, date, article violation (if identified), fine amount, May 2018 – March 2020

Country	Month, Year	Firm name (if identified)	Industry (if applicable)	Article(s) violated (if identified)	Fine (Euro)
<b>Austria</b>	July 2019	Private person	NA	6	11,000
<b>Austria</b>	August 2019	NA	Medical services	13, 37	50,000
<b>Austria</b>	October 2019	Austria Post	Newspaper	5	18,000,000
<b>Belgium</b>	September 2019	Merchant	NA	5	10,000
<b>Belgium</b>	December 2019	Website providing legal information	Legal services	6, 12, 13	15,000
<b>Bulgaria</b>	February 2019	NA	Telecom services	5, 6	27,100
<b>Bulgaria</b>	August 2019	National Revenue Agency	Government	32	2,600,000
<b>Bulgaria</b>	August 2019	DSK Bank	Banking services	32	511,000
<b>Cyprus</b>	March 2019	NA	Local newspaper	6	10,000
<b>Cyprus</b>	November 2019	Private doctor	Medical services	5, 6	14,000
<b>Denmark</b>	March 2019	Taxa 4X35	Transportation services	5	160,700
<b>Denmark</b>	June 2019	IDdesign A/S	Design services	5	200,850
<b>Denmark</b>	March 2020	Gladsaxe Municipality	Government	5, 32	14,000
<b>France</b>	January 2019	Google	Information services	6	50,000,000
<b>France</b>	June 2019	Uniontrad Company	Translation services	5, 12, 13	20,000
<b>France</b>	June 2019	Sergic	Real estate services	32	400,000
<b>France</b>	June 2019	Active Insurance	Insurance services	32	180,000
<b>France</b>	Nov-19	Futura Internationale	Information services	5, 6, 13, 14, 21	500,000
<b>Germany</b>	2018	NA	Banking services	6	50,000
<b>Germany</b>	2018	NA	NA	83, 33, 34	20,000
<b>Germany</b>	November 2018	Knuddels.de	Information services	32	20,000
<b>Germany</b>	2019	NA	NA	NA	80,000
<b>Germany</b>	August 2019	Online company	Information services	NA	200,000
<b>Germany</b>	September 2019	Delivery hero	Information services	15	195,407
<b>Germany</b>	October 2019	Unknown	Banking services	32	80,000
<b>Germany</b>	October 2019	Unknown	Medical services	32	80,000
<b>Germany</b>	October 2019	Deutsche Wohnen	Housing services	5, 25	14,500,000

## EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

<b>Germany</b>	December 2019	1&1 Telecom GmbH	Telecom services	32	9,550,000
<b>Germany</b>	December 2019	Raipdata GmbH	Information services	37	10,000
<b>Germany</b>	December 2019	Hospital	Medical services	32	105,000
<b>Greece</b>	July 2019	PwC	Consultancy services	83	150,000
<b>Greece</b>	October 2019	Telecom services provider	Telecom services	5, 25	200,000
<b>Greece</b>	October 2019	Telecom services provider	Telecom services	21, 25	200,000
<b>Greece</b>	December 2019	Aegan Marine Petroleum Network	Energy services	5, 6, 32	150,000
<b>Greece</b>	January 2020	Allseas Marine	Construction services	5	15,000
<b>Hungary</b>	April 2019	Political party	Government	33, 34	34,375
<b>Hungary</b>	May 2019	Event organizer	Event services	5, 6, 13	92,146
<b>Hungary</b>	2019	NA	NA	33	15,150
<b>Iceland</b>	March 2020	National Center of Addiction Medicine	Medical services	5, 32	20,600
<b>Ireland</b>	July 2019	State of Ireland	Government		
<b>Italy</b>	April 2019	M5S political party	Government	32	50,000
<b>Italy</b>	December 2019	Eni Gas e Luce	Energy services	5, 6, 17, 21	8,500,000
<b>Italy</b>	December 2019	Eni Gas e Luce	Energy services	5, 6	3,000,000
<b>Italy</b>	January 2020	Community of Francavilla Fontana	Government	5, 6	10,000
<b>Italy</b>	January 2020	Azienda Ospedaliero Universitaria Integrata di Verona	Medical services	5, 32	30,000
<b>Italy</b>	January 2020	Sapienza Università di Roma	University	5, 32	30,000
<b>Italy</b>	January 2020	TIM	Telecom services	5, 6, 17, 21	27,800,000
<b>Italy</b>	February 2020	RTI Reti Televisive Italiane	Information services	5, 6	20,000
<b>Lithuania</b>	May 2019	MisterTango UAB	Information services	5, 32, 33	61,500

## EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

<b>Netherlands</b>	July 2019	Haga Hospital	Medical services	32	400,000
<b>Netherlands</b>	October 2019	UWV	Insurance services	32	900,000
<b>Netherlands</b>	March 2020	Royal Dutch Tennis Association	Sports services	5, 6	525,000
<b>Norway</b>	April 2019	City of Bergen	Government	5, 32	160,400
<b>Norway</b>	February 2020	Raelingen Municipality	Government	5, 32	73,600
<b>Norway</b>	February 2020	Coop Finnmark SA	Grocery store	5, 6	36,800
<b>Poland</b>	March 2019	Data processor	Internet services	14	220,000
<b>Poland</b>	April 2019	Sports association	Sports services	6	12,950
<b>Poland</b>	September 2019	Morele.net	Internet services	32	644,780
<b>Portugal</b>	December 2018	Centro Hospitalar Barreiro Montijo	Medical services	51	400,000
<b>Romania</b>	July 2019	Unicredit Bank	Banking services	25	130,000
<b>Romania</b>	July 2019	Vreau Credit	Banking services	32	15,056
<b>Romania</b>	October 2019	Raiffeisen Bank	Banking services	32, 33	20,000
<b>Romania</b>	October 2019	World Trade Center Hotel	Hotel services	32	150,000
<b>Romania</b>	November 2019	Courier Services Company	Courier services	32	11,000
<b>Romania</b>	November 2019	ING Bank	Banking services	32	80,000
<b>Romania</b>	December 2019	S CNTAR TAROM SA	Transportation services	32	20,000
<b>Romania</b>	December 2019	Hora Credit IFN	Banking services	5, 25, 32, 33	14,000
<b>Spain</b>	June 2019	La Liga	Sports services	7	250,000
<b>Spain</b>	2019	Gestión de Cobros	Banking services	5	60,000
<b>Spain</b>	2019	Vodafone	Telecom services	5	27,000
<b>Spain</b>	2019	Endesa	Energy services	5	60,000
<b>Spain</b>	August 2019	Avon Cosmetics	Cosmetics	6	60,000
<b>Spain</b>	October 2019	Xfera Movilesa	Information services	5	60,000
<b>Spain</b>	October 2019	Vueling Airline	Transportation services	5, 6	30,000
<b>Spain</b>	October 2019	Madrileña Red de Gas	Energy services	32	12,000
<b>Spain</b>	November 2019	Vodafone España	Telecom services	6	60,000
<b>Spain</b>	November 2019	Corporacion Raditelevision Española	Information services	32	60,000

## EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities

<b>Spain</b>	November 2019	Xfera Movilesa	Information services	32	60,000
<b>Spain</b>	November 2019	Telefónica	Telecom services	5	30,000
<b>Spain</b>	November 2019	Viaqua Xestion Integral Auguas de Galicia	Water services	6	60,000
<b>Spain</b>	November 2019	Curenergía Comercializador de Último Recurso	Energy services	6	75,000
<b>Spain</b>	January 2020	Vodafone España	Telecom services	5	44,000
<b>Spain</b>	January 2020	EDP España	Concert services	6	75,000
<b>Spain</b>	January 2020	EDP Comercializadora	Concert services	6	75,000
<b>Spain</b>	January 2020	Asociacion de Medicos Democratas	Medical services	6	10,000
<b>Spain</b>	February 2020	Xfera Movilesa	Information services	5, 6	60,000
<b>Spain</b>	February 2020	Vodafone	Telecom services	5, 6	60,000
<b>Spain</b>	February 2020	Vodafone	Telecom services	5	50,000
<b>Spain</b>	February 2020	Iberia Lineas Aereas de Espana	Transportation services	5, 6, 21	20,000
<b>Spain</b>	February 2020	Vodafone	Telecom services	5, 6	75,000
<b>Spain</b>	February 2020	Vodafone	Telecom services	5, 6	75,000
<b>Spain</b>	February 2020	Iberdrole Clientes	Energy services	6	80,000
<b>Spain</b>	February 2020	Vodafone Espana	Telecom services	5, 32	42,000
<b>Spain</b>	February 2020	Xfera Movilesa	Telecom services	5, 32	30,000
<b>Spain</b>	February 2020	HM Hospitales	Medical services	5, 6	48,000
<b>Spain</b>	February 2020	Vodafone	Telecom services	32	48,000
<b>Spain</b>	March 2020	Telefónica	Telecom services	58	30,000
<b>Spain</b>	March 2020	Gesthotel Activos Balagares	Hotel services	5	15,000
<b>Spain</b>	March 2020	Vodafone	Telecom services	5, 6	24,000
<b>Spain</b>	March 2020	Vodafone	Telecom services	5, 6	40,000
<b>Spain</b>	March 2020	Vodafone	Telecom services	5, 32	42,000
<b>Spain</b>	March 2020	Vodafone	Telecom services	5, 6	60,000
<b>Sweden</b>	August 2019	Swedish School Board	Government	7	18,680
<b>Sweden</b>	December 2019	Nusvar AB	Information services	6	35,000
<b>Sweden</b>	March 2020	Google	Internet services	5, 6, 17	7,000,000

<b>United Kingdom</b>	July 2019	Marriott	Hotel services	33	112,000,000
<b>United Kingdom</b>	July 2019	British Airways	Transportation services	32	207,000,000
<b>United Kingdom</b>	December 2019	Doorstep Dispensaree	Medical services	32	320,000

Source: Authors' calculations based on data provided in GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed March 26, 2020).

## Appendix B

**Table B.1:** List of fines exceeding €10,000 and €100,000, by country (May 2018-March 2020)

Country	€10,000 fines	€100,000 fines	Total value of fines (€)	Country	€10,000 fines	€100,000 fines	Total value of fines (€)
Austria	3	1	18,061,000	Latvia	1	0	150,000
Belgium	2	0	25,000	Liechtenstein (EEA)	0	0	---
Bulgaria	3	2	3,138,100	Lithuania	1	0	61,500
Croatia	0	0	---	Luxembourg	0	0	---
Cyprus	2	0	24,000	Malta	0	0	---
Czechia	0	0	---	Netherlands	3	3	1,825,000
Denmark	3	2	375,550	Norway (EEA)	3	0	270,800
Estonia	0	0	---	Poland	3	2	877,730
Finland	0	0	---	Portugal	1	1	400,000
France	5	4	51,100,000	Romania	8	2	440,056
German DPAs	12	5	24,890,407	Slovakia	0	0	---
Greece	5	4	715,000	Slovenia	0	0	---
Hungary	3	0	141,671	Spain	35	1	1,907,000
Iceland (EEA)	1	0	20,600	Sweden	3	1	7,053,680
Ireland	0	0	---	United Kingdom	3	3	319,320,000
Italy	8	3	39,440,000				

Source: Authors' calculations gathered from GDPR Enforcement Tracker, [www.enforcementtracker.com](http://www.enforcementtracker.com) (accessed March 26, 2020). Notes: EEA countries are not EU member states. However, they do belong to the European Economic Area and are subject to GDPR.