EMERGING TRENDS FROM THE FIRST YEAR OF EU GDPR ENFORCEMENT

By Catherine Barrett

I. INTRODUCTION

This article is an overview and analysis of the implementation of General Data Protection Regulation (GDPR) since coming into effect on May 25, 2018; it offers a first-year snapshot focusing on an analysis of the provisions cited to support imposition of fines on GDPR violators. Based on this analysis, legal practitioners may be better able to project which European Union (EU) member countries may take a leading role in enforcement actions and levying future fines under the GDPR. This article may serve as guidance to entities doing business in the EU and to counsel representing EU-present entities. These findings suggest changes in behavior or business location that could reduce the likelihood and/or severity of GDPR fines.

During the first year of enforcement, the Data Protection Authorities (DPAs), the independent bodies charged with investigating and enforcing the GDPR, largely followed the European Commission (EC) guidelines for assessing violations and setting associated fines (see the Annex at the end of this article for a summary of EC guidelines DPAs use to assess fines). The guidelines were developed by the EC European Data Protection Board (EDPB), an independent body charged with the consistent application of data protection rules across the EU, and the 28 EU DPAs.

PAST GDPR FINES

A total of 15 EU Member States brought enforcement proceedings which resulted in the issuance of an estimated 91 fines (see Figure 1).[1] Not including an analysis of case law, the fines levied to date indicate EU DPAs are acting conservatively, generally imposing fines below the maximum allowable under the regulation. Even for more serious violations of data principles and rights, DPAs generally did not impose the maximum allowable fines. In the first year of enforcement, DPAs tend to issue fines in conjunction with corrective measures in what appears to be an attempt to encourage changes in attitude and behavior concerning the protection of personal data.[2]

Under the GDPR, there are two tiers of fines. The lower, tier one fines—up to €10 million or 2% of the firm's worldwide annual revenue from the previous financial year, whichever is higher—are applied for less severe infringements. Typically, violations of Articles 8, 11, 25–39, and 42–43 receive tier one fines.[3] These Articles generally address rules governing data collection, control, and processing (i.e., data collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction)[4]; certification bodies which are charged with certifying organizations; and monitoring bodies accredited to assess compliance with a code of conduct.

The higher, tier two fines—up to €20 million or 4% of the firm's worldwide annual revenue from the previous financial year, whichever amount is higher—are applied to more severe infringements. Generally, violations against Articles 5, 6, 7[5], 9, 12–22, and 44–49 warrant higher fines because these infringements "go against the very principles of the right to privacy and the right to be forgotten that are at the heart of the GDPR."[6]

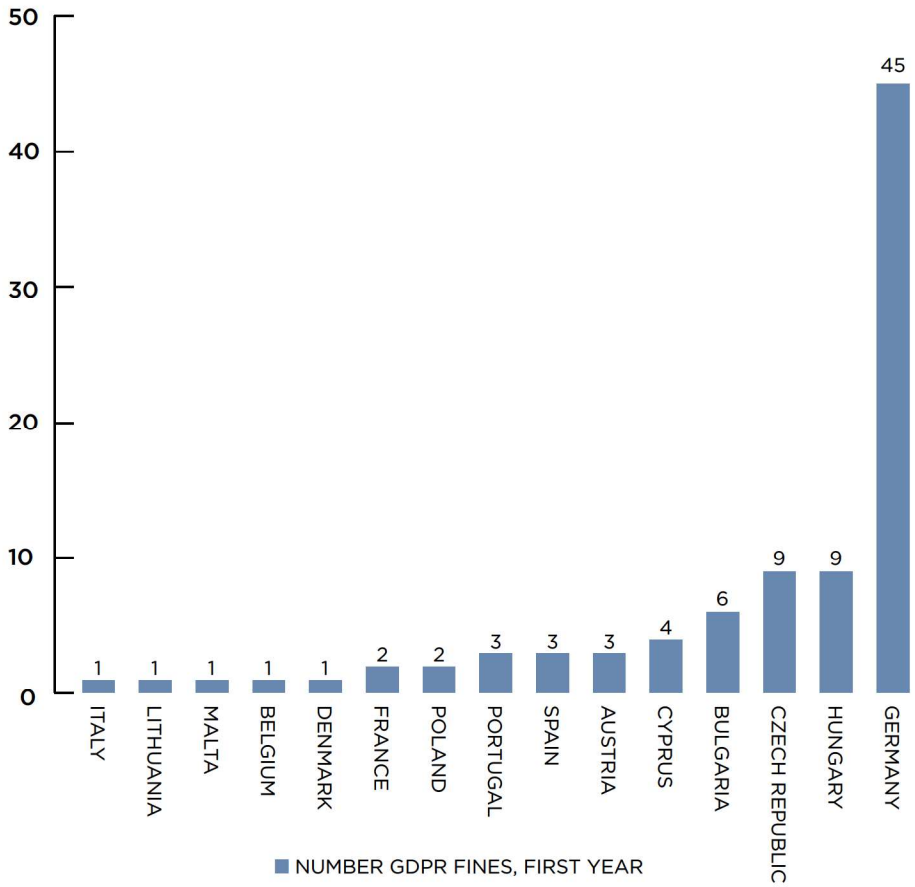
Germany, Hungary, the Czech Republic, Bulgaria, and Cyprus issued the most fines during the first year of GDPR enforcement. Of these countries, Germany issued more fines than any other EU Member State (~45) while France issued the highest fine (€50 million against Google).[7] In the coming years, DPAs from Germany, France, the United Kingdom (UK) and Ireland are likely to be among the most influential in terms of calculating and setting fines.[8] The sheer volume of multinational corporations headquartered and/or doing business in these countries suggests the fines issued by these DPAs will be precedent-setting.

FUTURE GDPR FINES

Importantly, in late 2015, the European Court of Justice (ECJ)—Europe's highest court—invalidated the US-EU Safe Harbor agreement between the EC and the U.S. Department of Commerce. The Safe Harbor agreement was succeeded by the Privacy Shield Framework in 2016 which, along with binding corporate rules and standard contract clauses, allowed for the legal transfer of EU resident personal data from the EU to the US.[9] However, "organizations that self-certified under the Privacy Shield are not GDPR compliant simply by virtue of their self-certification and must take additional steps to document their compliance with the GDPR."[10] Therefore, an organization that is certified under the Privacy Shield program may not be GDPR compliant and may be exposed to fines and other enforcement actions under the GDPR.

In the future, one country may emerge as the most influential DPA—Ireland. Ireland's Data Protection Commission (DPC) may play an outsized role among all EU DPAs for two reasons. Ireland is home to about a thousand, globally recognized US multinational companies across the financial, information and communication technology, and pharmaceutical industries.[11] Companies such as Google, Apple, Facebook, PayPal, Microsoft, Yahoo, eBay, AOL, Twitter, Intel Pfizer, Boston Scientific, Johnson & Johnson, Citigroup, BNY Mellon, State Street, BOA Merrill Lynch, Northern Trust, Goldman Sachs and J.P. Morgan all have a presence in Ireland.[12] DPC enforcement actions, therefore, will have an extraterritorial impact on some of the world's most recognized companies and serve as a model for how the GDPR should be enforced by other EU DPAs. As interpreted by more than one U.S. law firm, this expansive view of jurisdiction under the GDPR leads to the conclusion that a firm not located within the EU "will still be subject to the GDPR if it processes personal data of data subjects who are in the EU where the processing activities are related 'to the offering of goods or services' (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or 'the monitoring of their behavior' (Article 3(2)(b)) as far as their behaviour takes place within the EU."[13]

Figure 1 15 EU Member Countries Issued Fines in the First Year of GDPR Enforcement



II. REGULATORS FOCUSED ON FOUR ARTICLES TO SUBSTANTIATE MOST GDPR FINES

EU data regulators focused on four GDPR Articles, Articles 5, 6, 15, and 32, to substantiate the bulk of levied fines.[14] By far the most often cited was Article 5 (principles relating to processing of personal data). Article 5 principles include protecting personal data by ensuring appropriate levels of security to reduce the risk of unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality"). Article 5 also ensures personal data is collected in a limited manner, for a specific, explicit and legitimate purpose. Article 5 violations were cited an estimated 30 times from among the 91 fines levied.[15] Many regulators from across the EU found to Article 5 infringements such as failure to: process personal data lawfully, fairly, and in a transparent manner; prevent use of personal data for new purposes incompatible with the purpose for which the data were initially collected; delete personal data; and prevent indiscriminate access to an excessive number of user data.

In addition, Article 6 (lawfulness of processing) was the second most often cited infringement with a total of 12 violations. Under Article 6, lawful processing of personal data requires one (or more)

of the following six factors: (1) consent is obtained from the data subject; (2) data are processed in performance of a contract; (3) to comply with a legal obligation of the Member State or EU; (4) to protect vital interests (i.e., interests essential for the life of the data subject or for humanitarian purposes); (5) to perform a task that is in the public interest (i.e., a local government authority using personal data to collect taxes); or (6) where necessary to fulfill legitimate controller (individual or entity that determines the purpose and means of processing personal data, such as a payroll management company) or third-party interests.[16]

Articles 32 (security of processing personal data) and 15 (right of access by the data subject) were the third most often cited infringement with a total of 7 violations each. Under Article 32, for example, appropriate technical and organizational measures must be implemented to ensure security appropriate to the risk including, but not limited to, the pseudonymization and encryption of personal data. Article 15 provides a right of access whereby the data subject may request information about how personal data are being processed. Data subjects have a right to request a copy of data being processed, the purpose for processing the data, categories of data being processed (i.e., name, address, phone number) and any third-party recipients of the personal data, among others. Generally, regulators tend to levy fines for failures related to the lawful processing of personal data, including security measures to protect personal data.

III. 15 EU MEMBER STATES ISSUED FINES IN THE FIRST YEAR

Approximately 91 fines were imposed by 15 EU Member States in the first year.[17] Nearly half of Member States did not issue fines in the first year, many due to lack of sufficient resources.[18] As Figure1 illustrates, Germany, Hungary, the Czech Republic, Bulgaria, and Cyprus issued the most fines. Germany was the outlier among the EU Member States issuing an estimated 45 fines, five times more than Hungary and the Czech Republic (each issued nine fines).

IV. REGULATORS FOLLOW EC GUIDELINES IN APPLYING CARROTS AND STICKS

A review of the types of infringements and associated fines shows DPAs largely seek to use both the carrot and stick provided via GDPR. The DPAs—at this stage—want to change the perception of data protection, to view data as an asset to be protected. DPAs seek to change attitudes and behaviors via both compliance with the rules and, for egregious infringements, to apply the stick—the fine. One of the EC guiding principles is that fines should "adequately respond to the nature, gravity and consequences of the breach" and DPAs should "identify a corrective measure that is effective, proportionate and dissuasive."[19] Neither the guidelines nor Article 83 (general conditions for imposing administrative fines) define what is meant by "effective, proportionate and dissuasive," but the guidelines specify the DPA may consider whether to "reestablish compliance with the rules, or to punish unlawful behavior (or both)."[20] As a rule, DPAs did not issue maximum allowable fines. But, when they did, they tended to follow EC guidelines.

In accordance with the guidance, DPAs tend to apply higher fines when any one or more of four circumstances are present. First, where *the number of data subjects affected*, and subsequent level of damage, warrants it. For data beaches that are found, for example, to originate from "systemic breach or lack of adequate routines in place" and impact a number of data subjects, higher fines might be levied. For example, the Danish DPA issued a €161,000 fine against a Danish taxi company after an investigation found the company stored personal data of approximately nine million customers without a legitimate reason. Here, the number of data subjects impacted warranted a higher fine.

Second, if there are *several different infringements committed in any one particular case*, the DPA may impose a higher fine and/or prescribe corrective measures. For example, the DPA of France—the Commission Nationale de l'Informatique et des Libertés (CNIL)—characterized Google's data processing as "massive and intrusive in nature" and levied a €50 million fine against Google in part for violating multiple Articles: lack of transparency (Article 5), insufficient information (Articles 13 and 14) and lack of legal basis (Article 6). Though Google is appealing the decision before France's Supreme Administrative Court, the depth of the fine was in part substantiated by the breath of different infringements.

Third, *intentional acts or negligence trigger the possibility of higher fines*. The guidance specifies, for example, that "willful conduct on the data controller's part, or failure to take appropriate preventive measures, or inability to put in place the required technical and organizational measures" weigh in the DPA's assessment of the level of a fine. For example, the Portuguese DPA levied a €400,000 fine against a hospital as a result of failure to protect patient data, allowing hospital staff to indiscriminately access patients' data. The Portuguese DPA substantiated the fine by finding violations of three Articles: Article 5 for allowing indiscriminate access to an excessive number of users; Article 83 for violating basic data processing principles; and Article 32 for failing to ensure "continued confidentiality, integrity, availability and resilience of treatment systems and services" and failure to implement "measures to ensure a level of security adequate to the risk. . ."[21]

Fourth, *duration of an infringement* is another factor. For example, if data is exfiltrated as a result of a data breach and that data breach goes undetected for a long period of time, the length of time will likely be a factor in determining the damage to data subjects and resulting fine.

V. CONCLUSIONS AND FUTURE DIRECTION

The data supports the conclusion that DPAs largely followed the EC guidelines in assessing and levying fines during the first year of enforcement. Most of the fines were for violations of four Articles: 5, 6, 32, and 15. By far the most often cited was Article 5 (principles relating to processing of personal data). Article 6 (lawfulness of processing) was the second most often cited infringement. Articles 32 (security of processing personal data) and 15 (right of access by the data subject) were the third most often cited infringement.

Generally, violations against Articles 5, 6, 7, 9, 12–22, and 44–49 warrant higher fines because these infringements "go against the very principles of the right to privacy and the right to be forgotten that are at the heart of the GDPR."[22] However, in the first year of enforcement, fines were generally conservative and did not reach the maximum threshold. As more fines are levied, and some appealed through the courts, the guidelines will need to be updated to reflect current thinking on interpreting the enforcement provisions of the GDPR. For example, the outcome of the €50 million fine the French CNIL levied against Google will have an impact on how other DPAs assess and apply fines. The outcome of this case will also likely influence future guidance issued by the EC.

While only 15 EU Member States issued fines during the first year, the increase in DPA budgets and staff suggest many more Member States will be active in the coming years. Addressing data protection complaints, launching investigations, closing cases, levying fines and/or corrective action are resource-intensive activities. The European Data Protection Board shows France, Germany, Ireland, Italy, Poland and Spain have the largest staff to support their respective DPAs.[23] While budget and staff are not the only drivers of future GDPR fines, these well-resourced and staffed Member States are likely to be able to process complaints and issue fines more quickly than less-resourced countries. Of these, Ireland's DPC may play an outsized role among all EU because of the number of large US multinational corporations headquartered or doing business there. The breadth of fines issued by Ireland's DPC as well as the depth of investigative supporting evidence could serve as a roadmap for other EU DPA enforcement actions.

Figure 3 Guiding Principles for Assessing GDPR Fines

1	Infringement should result in "equivalent sanctions"
2	Administrative fines should be "effective, proportionate and dissuasive"
3	Individual assessments should be conducted on each case
4	Administrative fines should be harmonized across EU DPAs

ANNEX A: SUMMARY OF FOUR PRINCIPLES THAT SHAPE EC GUIDELINES DPAS USE TO ASSESS FINES

In October of 2017, the European Commission (EC) issued guidelines for DPAs to utilize when applying and setting GDPR fines.[24] The guidelines were developed by the EC European Data Protection Board (EDPB), an independent body charged with the consistent application of data protection rules across the EU, and the 28 EU DPAs. The guidelines include four principles that shape how the DPAs approach assessing fines:

1. Infringement should result in "equivalent sanctions"

This principle encourages DPAs to apply a consistent approach to their "use of corrective powers," including the "application of administrative fines in particular."[25] The EU member states want to "remove the obstacles to flows of personal data within the Union" by ensuring a standard of data protection across all 28 EU countries. The guidance specifies that while DPAs are independent and may choose corrective measures within their authority in accordance with Article 58, DPAs should avoid different corrective measures, including fines, for similar cases.

2. *Administrative fines should be "effective, proportionate and dissuasive"*

Fines should "adequately respond to the nature, gravity and consequences of the breach" and DPAs should "identify a corrective measure that is effective, proportionate and dissuasive. . ."[26] Neither the guidelines nor Article 83 define what is meant by "effective, proportionate and dissuasive," but the guidelines specify the DPA may consider whether to "reestablish compliance with the rules, or to punish unlawful behavior (or both)."[27]

3. Individual assessments should be conducted on each case

The GDPR requires an individual assessment of each case (Article 83). The DPA is charged with investigating complaints on a case-by-case basis within a reasonable period of time and in an impartial, fair manner. This principle calls on the DPA to "use a considered and balanced approach in their use of corrective measures, in order to achieve both an effective and dissuasive as well as a proportionate reaction to the breach" and "not to use them in a way which would devalue their effectiveness as a tool."[28] The EDPB issues a binding decision if disputes arise between authorities regarding the existence of an infringement.

4. *Administrative fines should be harmonized across EU member country DPAs*

In order to attain consistency, DPAs are directed to cooperate with each other and the EC "to support formal and informal information exchanges, such as through regular workshops." The purpose of the information exchange is to share the methodology used to formulate fines and the practice of applying fines to "achieve greater consistency" across the EU.

In addition to the guiding principles, DPAs are required to consider a number of factors under the GDPR when determining the scope and level of a fine. Article 58 details supervisory authority or DPA powers, including the imposition of administrative fines pursuant to Article 83. Article 83 is significant because it directs the DPA to consider many factors when determining the amount of a fine.

Catherine Barrett (cabarrett@mitre.org) is a cyber policy principal with MITRE in McLean, Virginia. She is the author of "Are the EU GDPR and the California CCPA Becoming the De facto Global Standards for Data Privacy and Protection?" (SciTech Lawyer, Spring 2019) and co-author of the book What Is . . . Telemedicine? (ABA, 2015). She received her JD/MBA from the American University Washington College of Law and is a (ISC)² Systems Security Certified Practitioner (SSCP). Approved

Continued on page 35

Continued from page 25

ENDNOTES

1. GDPR fines do not appear to be collected, organized, and reported publicly by the EC EDPB. Rather, private or nonprofit entities track and report fines issued by each EU Member State. This decentralized approach to tracking fines may, therefore, result in some variations of data.

2. Article 4(1) defines personal data as any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

3. Ben Wolford, *What Are the GDPR Fines?* GDPR.EU, https://gdpr.eu/fines (last visited Oct. 24, 2019).

4. *See* GDPR Article 4 for the full definition of data "processing."

5. Article 7 is focused on consent. Consent must be qualified under specific criteria in the article; where consent is provided by the data subject to process personal data, the data collector must be able to prove the individual or entity (i) obtained informed consent and (ii) that it was freely given by the data subject. In addition, the data subject has the right to withdraw consent at any time.

6. Ben Wolford, *What Are the GDPR Fines?*, https://gdpr.eu/fines.

7. In January of 2019 Google announced it would appeal the €50 million fine levied by French DPA (The Commission nationale de l'informatique et des libertés).

8. This assumes the UK stays in the EU.

9. United States Department of Commerce, International Trade Administration, "Privacy Shield Program Overview," https://www.privacyshield.gov/Program-Overview.

10. Stephan Grynwajc and Monica Meiterman-Rodriguez, Law Office of S. Grynwajc Blog, *Does the Privacy Shield Replace the GDPR?*, https://www.transatlantic-lawyer.com/2018/06/is-privacy-shield-a-substitute-to-complying-with-the-gdpr (June 13, 2018) (last visited Nov. 10, 2019).

11. Stephen Beard, *For Ireland, Multinational Companies Are a Blessing and a Curse,* MarketPlace.org (June 20, 2018), https://www.marketplace.org/2018/06/20/ireland-multinational-companies-blessing-and-curse.

12. David Purdue, Ireland National Treasury Management Agency (NTMA) Economics, Report Impacts of the US Economy on Ireland: A Quantitative and Qualitative Analysis (Aug. 2018), https://www.ntma.ie/uploads/publication-articles/Impacts-of-the-US-economy-on-Ireland-August-2018.pdf. Much of the rationale for the heavy US multinational presence can be traced to a decision in 2003 to peg the Irish corporate tax rate to 12.5% , which is about half the average of the 34 other countries in the Organization for Economic Cooperation and Development, and is less than the US corporate income tax rate of 21%. *See* Fred Lucas, *Ireland Lowered Its Corporate Tax Rate. Here's What Happened.* The Daily Signal (May 14, 2018), https://www.dailysignal.com/2018/05/14/ireland-lower-its-corporate-tax-rate-heres-what-happened.

13. DLA Piper, *Data Protection Laws of the World,* (Oct. 17, 2018), https://www.dlapiperdataprotection.com/index.html?t=law&c=FR&c2=DE.

14. *See* GDPR Enforcement Tracker, CMS Legal Servs., EEIG, https://www.enforcementtracker.com, and *The GDPR: One Year On*, Ius Laboris, https://theword.iuslaboris.com/hrlaw/insights/the-gdpr-one-year-on.

15. Data related to GDPR fines, including total number of fines issued and types of infringements, were estimated based on information publicly available as of October 2019. With regard to Germany, estimates are used to calculate total number of fines as well as types of infringements. The DPA (State Commissioner for Data Protection and Freedom of Information Baden-Württemberg (LfDI)) does not appear to maintain a publicly available, centralized database of GDPR fines issued by the State.

16. South Bank Legal Solicitors, *The GDPR – What Is Lawful Processing of Personal Data?,* http://www.southbanklegal.com/gdpr-lawful-processing-personal-data, (last visited Nov. 11, 2019).

17. Prakash (PK) Paran, Patrick Van Eecke, George Mortimer, James Clark Rick Masters, *GDPR Data Breach Survey: February 2019,* DLA Piper LLC (July 11, 2019), https://www.dlapiper.com/en/uk/insights/publications/2019/07/updated-guide-on-the-insurability-of-gdpr-fines-across-europe.

18. Croatia, Estonia, Finland, Greece, Ireland, Latvia, Luxembourg, Netherlands, Romania, Slovakia, Slovenia, Sweden, and the UK did not issue fined under GDPR during the first year of enforcement.

19. European Commission, *Id.*

20. European Commission, *Id.*

21. Ana Monteiro, *First GDPR Fine in Portugal Issued Against Hospital for Three Violations,* IAPP The Privacy Advisor (Jan. 3, 2019), https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations.

22. Ben Wolford, *What Are the GDPR Fines?*, https://gdpr.eu/fines.

23. European Data Protection Board, *First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities,* (last visited Oct. 22, 2019), https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/02/9_EDPB_report_EN.pdf. Note, the UK DPA (Information Commissioner) data did not appear in the EDPB report.

24. This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC, http6s://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

25. European Commission, *Article 29 Data Protection Working Party*: *Guidelines on the Application and Setting of Administrative Fines*, (Oct. 3, 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

26. European Commission, *Id.*

27. European Commission, *Id.*

28. European Commission, *Id.*