THE GDPR: A RETROSPECTIVE AND PROSPECTIVE LOOK AT THE FIRST TWO YEARS

Erin Hilliard†

I. INTRODUCTION

"The Clock Is Ticking: Is Your Company Ready for GDPR?"[1]

"Marriott Faces Massive $123 Million GDPR Fine For 2018 Security Breach"[2]

"General Data Protection Regulation (GDPR): What you need to know to stay compliant"[3]

For three years, these four letters, G-D-P-R, have been making headlines around the world. In May 2018, Google searches for the GDPR were more popular than searches for Beyoncé.[4] Consumers have received countless notifications from companies about their data collection practices. The new E.U. General Data Protection Regulation (GDPR or "Regulation") has made a significant impact on companies of all sizes and industries—but why?

The right to privacy, the protection of one's private and family life, home, and correspondence, has a longstanding history in Europe. Its origins can be

DOI: https://doi.org/10.15779/Z384J09Z3K

† J.D., 2021, University of California, Berkeley, School of Law. I would like to recognize the people who have been instrumental in the successful completion of this publication. I would like to express my sincere gratitude to Professor Chris Jay Hoofnagle for his valuable feedback and suggestions throughout the publication process. I would also like to acknowledge Professor Kenneth A. Bamberger and BCLT Executive Director Jim Dempsey for their critical assessments and encouragement during the drafting process. A huge thank you also goes out to Dr. Su Li for her statistical expertise.

1. *The Clock Is Ticking: Is Your Company Ready For GDPR?*, THE ONE BRIEF, https://theonebrief.com/the-clock-is-ticking-is-your-company-ready-for-gdpr/ (last visited May 18, 2020).

2. Nicole Lindsey, *Marriott Faces Massive $123 Million GDPR Fine For 2018 Security Breach*, CPO MAGAZINE (July 23, 2019), https://www.cpomagazine.com/data-protection/marriott-faces-massive-123-million-gdpr-fine-for-2018-security-breach/.

3. Michael Nadeau, *General Data Protection Regulation (GDPR): What You Need to Know to Stay Compliant*, CSO ONLINE (May 29, 2019), https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html.

4. Rachel Thompson, *GDPR is Currently Searched for More Than Beyoncé on Google*, MASHABLE (May 23, 2018), https://mashable.com/2018/05/23/google-trends-gdpr-beyonce/.

traced as far back as the European Convention on Human Rights,[5] enacted in 1953.[6] The right to data protection is recognized in Article 8 of the E.U. Charter of Fundamental Rights.[7] The E.U. Court of Justice often conflates the two rights, treating data protection as a subset of the right to privacy,[8] while some academics argue a distinction between the two is necessary.[9] Regardless of the specific terminology used, Europe's privacy protections are derived from these two rights and the GDPR is the result of a tremendous amount of iterative legislation on the part of the European Union and its member states to ensure the fundamental rights and freedoms of its citizens remain protected.[10]

Prior to proposing the GDPR, lawmakers recognized that technology had advanced exponentially since the Data Protection Directive—the data protection legislation preceding the GDPR—was written in 1995, and they were concerned the Directive no longer provided E.U. citizens with adequate protection.[11] Lawmakers also wanted to make data protection practices across the European Union more harmonious and consistent.[12] Now, with the GDPR in effect, hefty penalties of millions of euros,[13] a widened territorial scope of E.U. data protection law,[14] and compliance demands from vendors and partners have successfully motivated many companies into compliance.

5. Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR 3 (Sept. 15, 2014), https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en.

6. *Details of Treaty No.005*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005 (last visited May 12, 2020).

7. Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) and art. 8, 2010 O.J. (C 83).

8. Orla Lynskey, *Deconstructing Data Protection: The 'Added-value' of a Right to Data Protection in the EU Legal Order*, 36 INT'L & COMPARATIVE L.Q. 569, 597 (2014).

9. See*, e.g.*, *id.* (arguing a judicial recognition of the distinction is necessary because data protection provides individuals with more rights over more types of data than the right to privacy).

10. *See* Convention 108 and Protocols, COUNCIL OF EUROPE, https://www.coe.int/en/web/data-protection/convention108-and-protocol (last visited May 12, 2020); Hustinx, *supra* note 5, at 2, 4, 9, 29.

11. *Id.* at 26–27.

12. *Id.*

13. *Id.* at 33.

14. E.U. data protection law has expanded under the Regulation to encompass not only companies based in the European Union, but also companies who target or monitor the behavior of E.U. citizens. *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)—Version for Public Consultation*, EUROPEAN DATA PROTECTION BOARD (Nov. 16, 2018), https://edpb.eropa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf.

Privacy professionals are enjoying phenomenal job security. But has the GDPR achieved its goals? What did enforcement look like for the first two years?

The GDPR is an enormous and comprehensive regulation that affects thirty countries, each with its own unique culture, objectives, and needs. It took four years of negotiations for all parties subject to the Regulation to finally agree on a draft.[15] From the very beginning, the Article 29 Working Party (now the European Data Protection Board), which was charged with providing guidance on GDPR implementation, acknowledged that consistent implementation of the GDPR would require national supervisory authorities to work together on "sub-national, national and cross-border levels."[16]

In the first year of implementation, over 144,000 individual complaints and more than 89,000 data breach notifications were reported.[17] Countries have worked diligently to restructure and operationalize their methods for responding to and investigating E.U. citizens' complaints and company data breach notifications. Companies continue to navigate GDPR requirements, which were completely foreign to many organizations based outside of Europe. They seek guidance from European data protection authorities and E.U. institutions and advisory bodies regarding the interpretation and implementation of specific articles. While complete harmonization of data protection practices across thirty countries (twenty-seven E.U. member states and three European Economic Area (EEA) countries) may not be realistic, some of the early fragmentation in enforcement will become inconsequential with time.

Many practitioners and scholars have been looking to the number of imposed administrative fines across the European Union as a measure of overall "success" of the GDPR. Counting fines is an empirical way to track enforcement across countries. One way to assess the consistency of GDPR enforcement, a key goal of the new regulation, is to ask when, where, and why administrative fines were imposed during the first two years of GDPR enforcement. At this point in time, there are not any known academic

15. *See EU General Data Protection Regulation - Background*, DLA PIPER, https://www.dlapiper.com/en/portugal/focus/eu-data-protection-regulation/background/ (last visited May 12, 2020).

16. *Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679*, Article 29 Data Protection Working Party, 17 (Oct. 3, 2017) [hereinafter Article 29 Data Protection Working Party].

17. *GDPR One Year Anniversary—Infographic*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, https://iapp.org/resources/article/gdpr-one-year-anniversary-infographic/ (last visited May 12, 2020).

resources that have comprehensively tracked all fines across each E.U. member state and provided an empirical analysis of the data.

This Note addresses that gap in the literature. We have done an exhaustive search to identify all GDPR fines and nonmonetary sanctions—imposed or pending enforcement—across the E.U. member states, three EEA countries, and the United Kingdom for the time period May 25, 2018, the date of enactment, through March 31, 2020. (The United Kingdom withdrew from the European Union in January 2020,[18] but remained subject to the GPDR until December 2020,[19] and is therefore included in all analyses.) Our search yielded a total of 311 enforced fines and forty-nine pending actions across the thirty-one countries[20] where the GDPR was enforced during this time period. In this Note, we use descriptive statistics (mean, median, mode, range, and linear regression) to analyze the data and present our results, including noteworthy findings, patterns, and trends of enforcement since implementation.

The number of administrative fines imposed is increasing rapidly, and the median value of these fines is also increasing. In the first six months after the GDPR was enacted, fines were imposed in smaller numbers than expected. This may be because many underestimated how each country's micro-decisions regarding national privacy legislation and GDPR implementation would initially impact the harmonization of GDPR enforcement practices across the European Union. Two behaviors played a role: first, it was difficult for a country to impose fines for GDPR violations without having first passed national privacy legislation that includes the nation's selected GDPR derogations (discretionary articles), and second, countries with education or warning-first implementation approaches fined much less than countries who took active enforcement stances. However, the impact of these micro-decisions on fine consistency will decrease with time.

Looking at the 311 fines imposed in the first two years of enforcement, the total number and median fine value increased from 2018 to 2019. The number of fines issued increased nearly eightfold from 2018 (twenty-five fines) to 2019 (193 fines). In the first quarter of 2020 alone, ninety-three fines were issued. The median fine in 2018 was €3,200, while the median fine in 2019 was

18. The data set includes enforcement actions brought by the United Kingdom until it withdrew from the European Union in January 2020. *See generally Brexit: All You Need to Know About the UK Leaving the EU*, BBC (Feb. 17, 2020), https://www.bbc.com/news/uk-politics-32810887.

19. *Information Rights and Brexit Frequently Asked Questions*, INFORMATION COMMISSIONER'S OFFICE (May 20, 2020), https://ico.org.uk/for-organisations/data-protection-and-brexit/information-rights-and-brexit-frequently-asked-questions/.

20. The data set includes enforcement actions brought by the United Kingdom. *Id.*

€11,380, demonstrating that fine values are increasing but small fines are still more prevalent than massive fines. The median fine in the first quarter of 2020 (accounting for the first three months of the year) was €6,670, more than double the median fine in the seven months of 2018 following enactment.

This Note proceeds as follows. Part II explains the motivations behind the GDPR and provides an overview of key aspects of the GDPR that are crucial to assessing the enforcement actions that have occurred. Part III analyzes each country's enforcement behavior and GDPR implementation approach. Part IV presents the data, including a breakdown of fines by country and violation type, a comparison of total fines by country to gross domestic product, and a discussion of the industries most affected by enforcement actions. Part V discusses anticipated enforcement trends based on the data and findings presented in Parts III and IV.

II. BACKGROUND

A. WHAT IS THE GDPR?

The GDPR became enforceable on May 25, 2018.[21] Thirty countries—all twenty-seven E.U. member states and three EEA countries—are subject to the GDPR.[22] The protection of personal data is a fundamental right of all E.U. citizens, and the GDPR serves to enhance and unify data protection processes across Europe.[23] The GDPR defines personal data as "any information relating to an identified or identifiable natural person."[24] These identifiable, natural persons are referred to as "data subjects" throughout the Regulation.[25]

The GDPR has a laser focus on "[t]he protection of natural persons in relation to the processing of personal data."[26] Data "processing" is viewed as any operation(s) "performed on personal data [. . .] whether or not by automated means."[27] Unlike the GDPR's predecessor, the Data Protection

21. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Apr. 27, 2016), art. 99(2), 2016 O.J. (L 119), https://eur-lex.europa.eu/eli/reg/201 6/679/oj [hereinafter GDPR].

22. *GDPR National Implementation Legislation Tracker*, THOMSON REUTERS PRACTICAL LAW UK (Sept. 20, 2019), https://uk.practicallaw.thomsonreuters.com/w-013-1949 [hereinafter THOMSON REUTERS PRACTICAL LAW UK].

23. Charter of Fundamental Rights of the European Union (Oct. 26, 2012), art. 8(1), 2012 O.J. (C 326).

24. GDPR, *supra* note 21, art. 4(1).

25. *Id.*

26. *Id.* Recital 1; *see also id.* art. 94.

27. *Id.* art. 4(2).

Directive, the GDPR is a regulation that is wholly enforceable as law in each E.U. member state.[28] The Data Protection Directive placed obligations on individual member states to implement data protection laws locally.[29] In contrast, the GDPR provides one set of data protection rules that must be followed in each member state, with the exception of a number of derogations where articles can be tailored to, and supplemented by, national law.[30]

B. INTENT OF THE GDPR

The European Commission was particularly concerned that the lack of consistency regarding data protection standards across E.U. member states would hamper economic development.[31] In 1990, the Commission submitted a proposal for a directive that would create an E.U.-wide standard for personal data protection, making it easier for businesses to operate.[32] After four years of negotiations, the 1995 Data Protection Directive was adopted.[33] The overarching goals of the Directive were twofold: (1) to protect E.U. citizens' rights to privacy concerning the processing of personal information, and (2) to encourage development of the E.U. market by enabling the free flow of data.[34] The Directive led to more consistent data protection standards across countries than had previously existed.[35]

Over time, however, it became clear that the Directive needed to be updated. First and foremost, technology had evolved tremendously since the Directive became enforceable in 1998.[36] When the Directive was implemented, the internet was just taking off. Today, advanced technologies are a part of everyday life, and online monitoring and data collection are commonplace. The technological age presents new challenges that require more effective protections.[37] Second, implementation of the Directive varied greatly across

28. European Union, *Regulations, Directives and Other Acts*, OFFICIAL WEBSITE OF THE EUROPEAN UNION, https://europa.eu/european-union/eu-law/legal-acts_en [hereinafter European Union] (last visited May 12, 2020).

29. *Id.*

30. GDPR, *supra* note 21, Recital 10.

31. Hustinx, *supra* note 5, at 9.

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

36. *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, COMMISSION OF THE EUROPEAN COMMUNITIES (May 15, 2003), https://op.europa.eu/en/publication-detail/-/publication/ff783aa5-5770-42e8-bac3-917fe0a361d7/language-en [hereinafter COMMISSION OF THE EUROPEAN COMMUNITIES].

37. *Id.* at 26.

the then twenty-eight[38] E.U. member states.[39] Because the Directive had to be transposed into the national law of each country, there were discrepancies in interpretation, application, and implementation across the member states.[40] After six years of planning and negotiations, the GDPR was adopted in 2016, replacing the Directive that had been law for over two decades.[41]

While the GDPR's steep administrative fines have garnered a lot of public attention, the success of the GDPR largely depends on the Regulation's ability to adapt to new technologies. To secure compliance, lawmakers drafted laws they hoped would be flexible enough to stay relevant as technological innovation continues at a rampant pace.[42] The introduction of larger fines was just one of many key changes that occurred in data protection law with the implementation of the GDPR. Table 1 provides an overview of the key attributes of the previous law, the Data Protection Directive, and the current law, the GDPR.

38. The United Kingdom withdrew from the EU in January 2020. *See generally Brexit: All You Need to Know About the UK Leaving the EU*, BBC (Feb. 17, 2020), https://www.bbc.com/news/uk-politics-32810887.

39. *See* Katie McMullan*, Legislative* Framework, *in European Data Protection: Law and Practice*, 49, 52 (Eduardo Ustaran ed., 2018).

40. Hustinx, *supra* note 5, at 9, 24–25.

41. *The History of the General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited May 12, 2020).

42. GDPR, *supra* note 21, Recitals 6–7.

Table 1: Key Attributes of the Data Protection Directive and the GDPR

Data Protection Directive	General Data Protection Regulation
Date Adopted: October 24, 1995[43]	**Date Adopted:** April 27, 2016[44]
Year Enforceable: 1998[45]	**Date Enforceable:** May 25, 2018[46]
Geographical Scope: Data processors established in the territory, or using equipment established in the territory, of a country subject to the Directive[47]	**Geographical Scope:**[48] • Companies established in the EU • Companies established outside the EU, who offer goods or services to the EU, or monitor individuals in the EU
Implementation Process: Transposed into the national law of each country[49]	**Implementation Process:** Enforceable as law in all EU member states[50]
Goals:[51] • Protection of fundamental privacy rights • Development of the EU market • Harmonization of data protection practices across countries	**Goals:**[52] • Update data protection law to account for technological innovation • Harmonization of data protection practices across countries

43. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 [hereinafter Directive 95/46/EC] (last visited May 12, 2020).
44. GDPR, *supra* note 21.
45. COMMISSION OF THE EUROPEAN COMMUNITIES, *supra* note 36, at 19.
46. GDPR, *supra* note 21, art. 99.
47. Directive 95/46/EC, art. 4.
48. GDPR, *supra* note 21, arts. 3(1)–(3).
49. Directive 95/46/EC, art. 4.
50. GDPR, *supra* note 21, Recital 10.
51. Hustinx, *supra* note 5, at 9.
52. *Id.* at 26–27.

Table 1 (continued): Key Attributes of the Data Protection Directive and the GDPR

New Requirements Under the GDPR[53]
• Now applies to all companies engaging with the EU market • Data subject right to Data Portability • Consent and explicit consent require affirmative action • 72 hours to notify regulator of a data breach • Appointment of Data Protection Officers in companies • Much larger, standardized administrative fines

C. DATA PROTECTION AUTHORITIES

Data protection authorities (DPAs), also referred to as supervisory authorities, are key supervisors and enforcers of the GPDR. DPAs are independent regulators[54] who are designated by member states to monitor the implementation of the GDPR and enforce penalties. Article 58(1) grants DPAs three types of power: investigatory, corrective, and advisory. Their investigatory powers include the ability to access all evidence necessary to fulfill their responsibilities and start investigations.[55] DPA corrective powers are vast and range from issuing reprimands to imposing administrative fines; they can even ban an organization's data processing activities.[56] DPA advisory powers concern advising companies when consulted, and the ability to issue, adopt, and approve codes of conduct and certifications.[57] DPAs use their powers to fulfill their tasks (enumerated in Article 57), which include handling complaints, carrying out investigations, promoting awareness of data protection, and cooperating with other nations to ensure consistent application of the Regulation.[58] Some countries have one DPA while other countries have many. When a country has more than one DPA, as is the case in Germany, that member state must ensure consistency across all of its national DPAs.[59] Although member states had already appointed DPAs under the Data

53. *EU General Data Protection Regulation—Key Changes*, DLA PIPER, https://www.dlapiper.com/en/portugal/focus/eu-data-protection-regulation/key-changes/#wider%20territorial%20scope (last visited May 17, 2020).

54. GDPR, *supra* note 21, art. 52(1).

55. *Id.* art. 58(1).

56. *Id.* art. 58(2).

57. *Id.* art. 58(3).

58. *Id.* art. 57.

59. *Id.* art. 51(3).

Protection Directive,[60] DPAs now have significantly larger caseloads as a result of the GDPR's broader territorial scope and more serious penalties.

Although this Note focuses heavily on the role DPAs play in enforcement, specifically their power to issue administrative fines, it is important to note that DPAs are not the only enforcement mechanism available under the Regulation. Individuals can pursue legal action in accordance with their country's national laws.[61] Industry self-regulation is another enforcement tool the GDPR advances through the data processing accountability requirement (Table 2), the mandated appointment of Data Protection Officers within organizations,[62] and the creation of codes of conduct and data protection certification processes.[63]

D. GDPR DATA PROCESSING PRINCIPLES

Article 5(1) of the GDPR sets out seven data processing principles that inform the purpose and intent of the legislation (Table 2). These principles are similar to the principles of the Data Protection Directive, with the exception of the Accountability principle, which is new under the GDPR.[64] These seven data processing principles "embody the spirit" of the GDPR.[65] The highest tier of administrative fines can be imposed for violating these principles.[66] Fines are administered by member state DPAs[67] (or the European Data Protection Supervisor, if the suspected GDPR violator is an E.U. institution)[68] using both the text of the Regulation and interpretation guidance from E.U. advisory bodies.[69] Below is a brief explanation of each guiding principle. Recitals, while not binding, are used in legal documents to explain the reasoning behind certain terms and decisions. Recital 39 provides important context for how to interpret and follow the seven Article 5(1) data processing principles.

---

60. Detlev Gabel and Tim Hickman, *Chapter 14: Data Protection Authorities—Unlocking the EU General Data Protection Regulation*, WHITE & CASE (Apr. 5, 2019), https://www.whitecase.com/publications/article/chapter-14-data-protection-authorities-unlocking-eu-general-data-protection.

61. GDPR, *supra* note 21, art. 79.

62. *Id.* art. 37.

63. *Id.* arts. 40–43.

64. *The Principles*, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (last visited May 12, 2020).

65. *Id.*

66. GDPR, *supra* note 21, art. 83(5)(a).

67. *Id.* art. 83(1).

68. *Complaints*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/node/75_en (last visited May 1, 2020).

69. *See* Article 29 Data Protection Working Party, *supra* note 16.

Table 2: Data Processing Principles

Article 5(1)[70]	Recital 39 Explanation[71]
(a) "[L]awfulness, [F]airness and [T]ransparency"	"Any processing of personal data should be lawful and fair." "It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed." "Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing."
(b) Purpose Limitation	"[T]he specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data."
(c) Data Minimization	"The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed."
(d) Accuracy	"Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted."

70. GDPR, *supra* note 21, art. 5.
71. *Id.* Recital 39.

Table 2 (continued): Data Processing Principles

Article 5(1)	Recital 39 Explanation
(e) Storage Limitation	"[It must be ensured] that the period for which the personal data are stored is limited to a strict minimum." "In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review."
(f) Integrity and Confidentiality	"Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing."
Article 5(2)[72]	**Article Text**
Accountability	"The controller[73] shall be responsible for, and be able to demonstrate compliance with, paragraph 1."

E. DATA SUBJECT RIGHTS

Chapter three of the GDPR enumerates seven rights that data subjects can exercise under the Regulation. These rights are listed in Table 3. The largest possible fines can also be imposed for infringement of these rights.[74]

72. GDPR, *supra* note 21, art. 5.

73. "'[C]ontroller' means 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." GDPR, *supra* note 21, art. 4(7).

74. *Id.* art. 83.

Table 3: Data Subject Rights

Article 15[75]	**Recital 63 Explanation**[76]
Right of Access	"A data subject should have the right of access to personal data which have been collected concerning him or her."
Article 16[77]	**Article Text**
Right to Rectification	The right to "obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her[,]" including the right to complete personal data that is "incomplete."
Article 17[78]	**Recital 65 Explanation**[79]
Right to Erasure	"In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation."

75. *Id.* art. 15.
76. *Id.* Recital 63.
77. *Id.* art. 16.
78. GDPR, *supra* note 21, art. 17.
79. *Id.* Recital 65.

Table 3 (continued): Data Subject Rights

Article 18[80]	**Recital 67 Explanation**[81]
Right to Restriction of Processing	"Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website."
Article 20[82]	**Article Text**
Right to Data Portability	"[T]he right to receive [] personal data" that a data subject "has provided to a controller, in a structured, commonly used and machine-readable format and [] the right to transmit those data to another controller without hindrance." Also, "the right to have personal data transmitted from one controller to another [controller], where technically feasible."
Article 21[83]	**Article Text**
Right to Object	A data subject's right to object, "at any time to processing of personal data concerning him or her."
Article 22[84]	**Recital 71 Explanation**[85]
"[R]ight [N]ot to [B]e [S]ubject to a [D]ecision [B]ased [S]olely on [A]utomated [P]rocessing"	"The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her."

80. *Id.* art. 18.
81. *Id.* Recital 67.
82. *Id.* art. 20.
83. GDPR, *supra* note 21, art. 21.
84. *Id.* art. 22.
85. *Id.* Recital 71.

Companies should have mechanisms in place for data subjects to exercise these rights and request, access, obtain, rectify, or erase their data.[86] These company mechanisms and expectations are further explained in Articles 12, 13, 14, and 19. Companies are expected to respond "without undue delay" to data subject requests, within one month at the latest.[87] This can be an operationally difficult requirement for many companies to meet, especially very small and very large companies where the cost of compliance is significant, for the former in terms of budget and the latter in terms of sheer scale.

F. WHY THE GDPR AFFECTED COMPANY BEHAVIOR ACROSS THE WORLD

Almost all modern businesses are affected by the GDPR because the law defines relevant data processing so broadly. A business can be subject to GDPR compliance even when the business is not physically present in the European Union. Two provisions in particular might ensnare a U.S. business: if it monitors Europeans or if it offers goods or services to Europeans. Failure to comply with the GDPR can trigger heavy fines.

The GDPR applies to data processing activities in three contexts:

(1) A company is established in the European Union (regardless of where the data processing actually takes place);[88] or

(2) A company is not established in the European Union, but its data processing activities include "the offering of goods or services" or the monitoring of E.U. citizens within the European Union;[89] or

(3) A company is established in a place where E.U. member state law applies.[90]

Recital 23 provides some guidance regarding what constitutes "offering goods and services" to E.U. citizens. While mere accessibility of a website or use of a member state language on a website is insufficient, actions such as using the language and currency of a member state on a website with the possibility of ordering goods and services in that language could be viewed as targeting individuals within the European Union and weigh in favor of required GDPR compliance.[91] Because of the broad territorial scope of the Regulation, the threat of massive fines for noncompliance, and the fear of

86. *Id.* Recital 59.
87. *Id.*
88. GDPR, *supra* note 21, art. 3(1).
89. *Id.* art. 3(2)(a).
90. *Id.* art. 3(3).
91. *Id.* Recital 23.

losing access to the entire European market, many companies not established in the European Union have felt pressure to comply with the GDPR.[92]

Furthermore, the Regulation applies to a variety of business processes that are commonplace in our technological age. Any company that processes personal data "wholly or partly by automated means" or has information that forms (or is intended to form) a nonautomated filing system must comply with GDPR data protection standards, provided that the company's activities are within the territorial scope of the Regulation (explained above).[93] Purely personal or household activities are exempt, and there are limited exceptions for micro, small, and medium-sized enterprises.[94] However, the material scope of the Regulation remains broad, with the goal of achieving a consistent level of protection for European consumers across business sectors and industries.[95]

G. GDPR ADMINISTRATIVE FINES

The GDPR changed the way data protection law is implemented across the European Union and also significantly increased sanctions for noncompliance. Companies are now facing heightened compliance requirements that, if violated, can result in massive monetary penalties. The GDPR has generated a huge shift in the relative importance of data protection law when compared to the trivial fines that were administered under the Data Protection Directive.[96] The risk of such severe penalties has forced companies to prioritize GDPR compliance.

There are two categories of fines: a higher category and a lower category.[97] The highest fine category, outlined in GDPR Article 83(5), sets a maximum fine of €20 million or four percent of a company's total worldwide turnover and can be imposed for violating:

- "Basic principles [of data] processing";
- "[D]ata subjects' rights";

92. *See, e.g.*, Ivana Kottasova, *These Companies Are Getting Killed by GDPR*, CNN BUSINESS (May 11, 2018), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html; Daniel Mikkelsen, Henning Soller, Malin Strandell-Jansson & Marie Wahlers, *GDPR Compliance Since May 2018: A Continuing Challenge*, MCKINSEY & COMPANY (July 2019), https://www.mckinsey.com/business-functions/risk/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge.

93. GDPR, *supra* note 21, art. 2(1).

94. *Id.* art. 2(2).

95. *Id.* Recital 13.

96. *See* Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, INFO. & COMM. TECH. L., 28:1, 94 (Feb. 10, 2019), https://www.tandfonline.com/doi/full/10.1080/13600834.20 19.1573501.

97. GDPR, *supra* note 21, arts. 83(4)–(5).

- International data transfer processes;
- Member state law regarding the processing of specific types of data; and
- Orders from a Supervisory Authority.[98]

The lesser category of fines, found in Article 83(4), sets a maximum fine of €10 million or two percent of a company's total worldwide turnover, and applies to violations of:

- "[O]bligations of [] controller[s] and [] processor[s]";
- "[O]bligations of [] certification bod[ies]"; and
- "[O]bligations of [a] monitoring body."[99]

Data Protection Authorities are not required to impose fines for infringement of the GDPR.[100] They have the power to choose the most appropriate corrective measures in each instance.[101] Corrective measures may include, but are not limited to, warnings, reprimands, fines, banning data processing, and ordering that data breach notifications be sent to data subjects.[102]

When a DPA does elect to impose an administrative fine for GDPR infringement, there are four guiding principles that should be considered.[103] First, administrative fines should be equivalent across member states.[104] Similar fines should be imposed for similar violations.[105] Article 83(2) provides eleven criteria that shall be given "due regard" when deciding whether to impose a fine, and determining the amount of the fine.[106] Second, corrective measures (including fines) should be "effective, proportionate and dissuasive."[107] DPAs must assess all the facts of a case in a consistent and objective manner, and respond adequately to the severity of the infringement.[108] The Article 29 Working Party guidelines suggest that this "effective, proportionate and dissuasive" standard will be more precisely defined through practice and future case-law.[109] Third, each case must be assessed individually, starting with the

98. *Id.* art. 83(5).
99. *Id.* art. 83(4).
100. Article 29 Data Protection Working Party, *supra* note 16, at 6–8.
101. GDPR, *supra* note 21, Recital 148.
102. *Id.* art. 58(2).
103. Article 29 Data Protection Working Party, *supra* note 16, at 5–8.
104. GDPR, *supra* note 21, Recital 11.
105. Article 29 Data Protection Working Party, *supra* note 16, at 5.
106. GDPR, *supra* note 21, art. 83(2).
107. *Id.* art. 83(1).
108. Article 29 Data Protection Working Party, *supra* note 16, at 6.
109. *Id.* (emphasis removed).

Article 83(2) fine considerations.[110] Finally, DPAs are expected to cooperate with one another and the European Commission, through formal and informal means, to achieve a harmonized approach to administrative fines.[111]

Fines should be used as an effective tool, neither overused nor viewed as a last resort.[112] Individual countries can choose whether or not to apply the Article 83 administrative fine structure to public authorities and bodies established in that country.[113] When a country's legal system does not allow for administrative fines, as is the case in Denmark and Estonia, Article 83 can be applied to initiate and impose a fine.[114] Some countries have specified when certain corrective measures will be used. In Austria, for example, first-time infringers are only issued a warning.[115]

With an understanding of the goals and compliance requirements of the GDPR, Parts III through V will now present an empirical analysis of the administrative fines that have been imposed thus far. Part III analyzes each country's enforcement behavior and GDPR implementation approach. Part IV presents the data, including a breakdown of fines by country and violation type, a comparison of total fines by country to gross domestic product, and a discussion of the industries most affected by enforcement actions. Part V discusses anticipated enforcement trends based on the data and findings presented in Parts III and IV.

III. A COMPARISON OF THE APPROACHES TAKEN ACROSS THE EU TO IMPLEMENT AND SUPPLEMENT THE GDPR

As a regulation, the GDPR became immediately enforceable as law, in what was then twenty-eight E.U. member states,[116] on May 25, 2018,[117] but member states implemented the Regulation through their own national privacy legislation in order to incorporate permitted country-specific alterations to the core text of the GDPR. The GDPR was incorporated into the EEA Agreement and enacted in Iceland, Norway, and Lichtenstein, the three EEA

110. *Id.* at 6–7.

111. *Id.* at 8.

112. *Id.* at 7.

113. GDPR, *supra* note 21, art. 83(1).

114. *GDPR Member State Permitted Variations and Requirements Chart: Overview*, THOMSON REUTERS PRACTICAL LAW UK, https://uk.practicallaw.thomsonreuters.com/w-012-6272 (last visited May 19, 2020).

115. *The GDPR: One Year On,* IUS LABORIS (May 24, 2019), https://theword.iuslaboris.com/hrlaw/insights/the-gdpr-one-year-on.

116. European Union, *supra* note 28.

117. GDPR, *supra* note 21, art. 99.

countries not part of the European Union, on July 6, 2018.[118] While enforceable as law, the GDPR allows for a number of derogations where member states can exercise discretion over how specific articles are applied.[119] These derogations include the option to lower the age of consent from sixteen years to no lower than thirteen years of age,[120] introduce further limitations on the processing of health data,[121] and retain certain data processing laws that member states may already have in place.[122] Member states were given the ability to restrict and supplement specific GDPR articles through derogations in order to ensure national and public security, as well as to safeguard other member state interests.[123] As a result, countries adopted their own national data privacy legislation which included nation-specific alterations to the core text of the GDPR.[124] Some member states released updated privacy laws quickly, while other member states did not implement the GPDR into their national privacy legislation until well into 2019.[125] For example, the United Kingdom's national Data Protection Act 2018 became enforceable the same day as the GDPR: May 25, 2018.[126] The United Kingdom's Data Protection Act is closely related to the GDPR, using the GDPR as a baseline and extending GDPR principles to additional data processing scenarios through derogations.[127] As illustrated in Table 4, twelve member states (approximately thirty-nine percent) implemented their own national privacy legislation by the GDPR enforcement date of May 25, 2018. The remaining countries implemented their legislation

118. THOMSON REUTERS PRACTICAL LAW UK, *supra* note 22.

119. Andrew Clearwater and Brian Philbrook, *GDPR Derogations and How to Prepare for Member State Variation*, CPO MAGAZINE (Sept. 29, 2017), https://www.cpomagazine.com/data-protection/gdpr-derogations-prepare-member-state-variation/.

120. GDPR, *supra* note 21, art. 8(1).

121. *Id.* art. 9(4).

122. Andrew Clearwater and Brian Philbrook, *GDPR Derogations and How to Prepare for Member State Variation*, CPO MAGAZINE (Sept. 29, 2017), https://www.cpomagazine.com/data-protection/gdpr-derogations-prepare-member-state-variation/.

123. GDPR, *supra* note 21, Recital 73.

124. *See GDPR Genius—Chapter 1 - General Provisions: Nation-Specific Notes*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (2019), https://iapp.org/resources/tools/gdpr-genius-chapter-1/.

125. *See Data Protection Laws of the World*, DLA PIPER (Jan. 2020), https://www.dlapiperdataprotection.com/.

126. *Data Protection Laws of the World—United Kingdom*, DLA PIPER (Jan. 14, 2020), https://www.dlapiperdataprotection.com/?t=law&c=GB.

127. Dan Swinhoe, *GDPR vs UK Data Protection Act 2018: What's the difference?*, CSO ONLINE (Aug. 5, 2019), https://www.csoonline.com/article/3410039/gdpr-vs-uk-data-protection-act-2018-whats-the-difference.html.

later in 2018, with nine countries not implementing national privacy legislation until 2019.[128] Slovenia has yet to pass local privacy legislation post-GDPR.[129]

Countries also had discretion over their GDPR implementation approach regarding how quickly and heavily they fined violators. Some countries were slow to fine, prioritizing education regarding proper GDPR implementation and delaying penalization for infringements. For example, Hungary's Data Protection Act requires its DPA to only issue warnings to companies who violate the Regulation for the first time.[130] In contrast, the Lithuanian DPA took a more active approach, announcing in January 2019 a list of seventy-five organizations it planned to inspect for GPDR compliance that year.[131]

To understand the different implementation approaches used, we assessed each country's approach to GDPR enforcement and categorized it as vigorous, progressing, or cautious based on the country's implementation approach, the total number of fines issued as of March 31, 2020, the cumulative total of all fines imposed, and the date when national privacy legislation was enacted (Table 4). Vigorous countries actively fined companies for violations, imposed a high number of fines or a few extremely large fines, and implemented their national privacy legislation before or near the date the GDPR became enforceable. In contrast, cautious countries were warning or education-first focused, imposed relatively few fines, and frequently enacted national privacy legislation later than the majority of E.U. member states. Progressing countries were countries with a combination of vigorous and cautious attributes. Based on these metrics, the five countries considered vigorous as of March 2020 were France, Germany, Italy, Spain, and the United Kingdom. Of the remaining twenty-six countries, thirteen (forty-two percent) were evaluated to be progressing, and thirteen (forty-two percent) were deemed cautious in their GDPR implementation approach.

The analysis presented in Table 4 was done twice in the process of writing this Note, once in May 2019 and again in March 2020. Both analyses used the same assessment factors. In May 2019, only four countries were categorized as vigorous. Italy moved from progressing to vigorous after it imposed a few large fines from May 2019 to March 2020, increasing its cumulative fine total from €50,000 to €39,454,946 (third only to the United Kingdom and France).

128. *See* THOMSON REUTERS PRACTICAL LAW UK, *supra* note 22.

129. *Data Protection Laws of the World—Slovenia*, DLA PIPER (Jan. 15, 2021), https://www.dlapiperdataprotection.com/index.html?t=law&c=SI.

130. *Data Protected—Hungary*, LINKLATERS (Nov. 2018), https://www.linklaters.com/en-us/insights/data-protected/data-protected---hungary.

131. Neil Hodge, *GDPR Enforcement Varies Widely by Country*, COMPLIANCE WEEK (July 19, 2019), https://www.complianceweek.com/gdpr/gdpr-enforcement-varies-widely-by-country/27436.article.

Five counties transitioned from cautious in May 2019 to progressing in March 2020: Austria, Hungry, the Netherlands, Romania, and Sweden. The Austrian privacy advocacy organization, None of Your Business, has been incredibly active in filing actions against companies for GDPR violations, moving Austria from the cautious to progressing category. Hungary's cumulative fine total more than doubled from May 2019 to March 2020, and Romania's total fine count increased fivefold in that period of time. Sweden imposed a few massive fines, increasing its cumulative fine total by more than €7,000,000. Similarly, the Netherlands both doubled its fine count and its cumulative fine total, warranting a progressing categorization. Lithuania, on the other hand, stated an intent to begin over seventy-five investigations in 2019,[132] but no evidence of additional sanctions, monetary or nonmonetary, were found. Therefore, Lithuania was recategorized from progressing to cautious.

132. Neil Hodge, *GDPR Enforcement Varies Widely by Country*, COMPLIANCE WEEK (July 19, 2019), https://www.complianceweek.com/gdpr/gdpr-enforcement-varies-widely-by-country/27436.article.

Table 4: Country Approach & Implementation Date of Nat'l Privacy Legislation

May 25, 2018-March 31, 2020

Country	Approach May 2019 (12 Months)	2017	2018												2019												2020			Approach March 2020 (23 Months)
		Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	
Austria																														
Belgium																														
Bulgaria																														
Croatia																														
Cyprus																														
Czech Republic																														
Denmark																														
Estonia																														
Finland																														
France																														
Germany																														
Greece																														
Hungary																														
Iceland																														
Ireland																														
Italy																														
Latvia																														
Liechtenstein																														
Lithuania																														
Luxembourg																														
Malta																														
Netherlands																														
Norway																														
Poland																														
Portugal																														
Romania																														
Slovakia																														
Slovenia																														
Spain																														
Sweden																														
United Kingdom																														

Vigorous Approach
Progressing Approach
Cautious Approach
GDPR Implementation Date
Implementation Date by Country

IV. A CLOSER LOOK AT GDPR FINES: GROWTH RATES, VIOLATION TYPES, QUANTITY BY COUNTRY AND ECONOMIC SECTOR

A. METHODS

To understand the GDPR enforcement landscape, we performed an exhaustive search to identify all fines and nonmonetary sanctions imposed and pending in the European Union as a result of the Regulation. This included an internet review of GDPR enforcement actions from May 25, 2018, the date of enactment, through March 31, 2020. We assembled a dataset of publicly available fines and nonmonetary sanctions for all twenty-seven E.U. member states, the United Kingdom, and three EEA—Lichtenstein, Iceland, and Norway—which are also subject to the GDPR.[133] Key sources included the CMS GDPR Enforcement Tracker,[134] Linklaters' Data Protected tracker,[135] DLA Piper's Data Protection Laws of the World Handbook,[136] PwC's Global Privacy and Security Enforcement Tracker,[137] Nathan Trust's GDPR Fines and Penalties News Feed,[138] Bird & Bird's GDPR Tracker,[139] None of Your Business's GDPRhub,[140] and country-specific DPA Annual Reports. News articles, Bloomberg Law resources, Thomson Reuters Practical Law charts, and European Data Protection Board (EDPB) reports were also examined. While every attempt was made to be comprehensive, the data sources are public information and impacted by variations in reporting, timeliness, and consistency.

Our search strategy yielded a total of 311 enforced fines and forty-nine pending actions across thirty-one countries for the time period of May 25, 2018, through March 31, 2020. We collected numerous data elements about each enforcement action, including imposed or pending status, fine amount,

133. THOMSON REUTERS PRACTICAL LAW UK, *supra* note 22.

134. GDPR Enforcement Tracker, CMS, https://enforcementtracker.com/ (last visited Mar. 31, 2020).

135. *Data Protected Home: Your Global Guide to Data Protection*, LINKLATERS, https://www.linklaters.com/en/insights/data-protected/home (last visited March 31, 2020).

136. *Data Protection Laws of the World*, DLA PIPER (Jan. 2020), https://www.dlapiperdataprotection.com/.

137. *Global Privacy and Security Enforcement Tracker*, PWC (2018), https://www.pwc.com/gx/en/issues/regulation/general-data-protection-regulation/hot-topics/enforcement-tracker.html.

138. *GDPR Fines and Penalties*, NATHAN TRUST, https://www.nathantrust.com/gdpr-fines-penalties (last visited Mar. 31, 2020).

139. *GDPR Tracker*, BIRD & BIRD, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker (last visited Mar. 31, 2020).

140. *GDPRhub*, NONE OF YOUR BUSINESS, https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub (last visited Mar. 31, 2020).

company, date of decision, and type of violation. Country-specific information such as gross domestic product (GDP), local privacy legislation implementation date, and GDPR enforcement approach were also included in the data set. We conducted quantitative analyses using descriptive statistics (mean, median, mode, range, linear regression) and used data visualization tools to create graphs that summarized our findings.

Not all countries' records are publicly available, and many DPAs only release annual reports. We have attempted to use the most up-to-date records and sources available, but it is possible that some of the reported information used to create the data set is outdated or incomplete due to collection limitations.

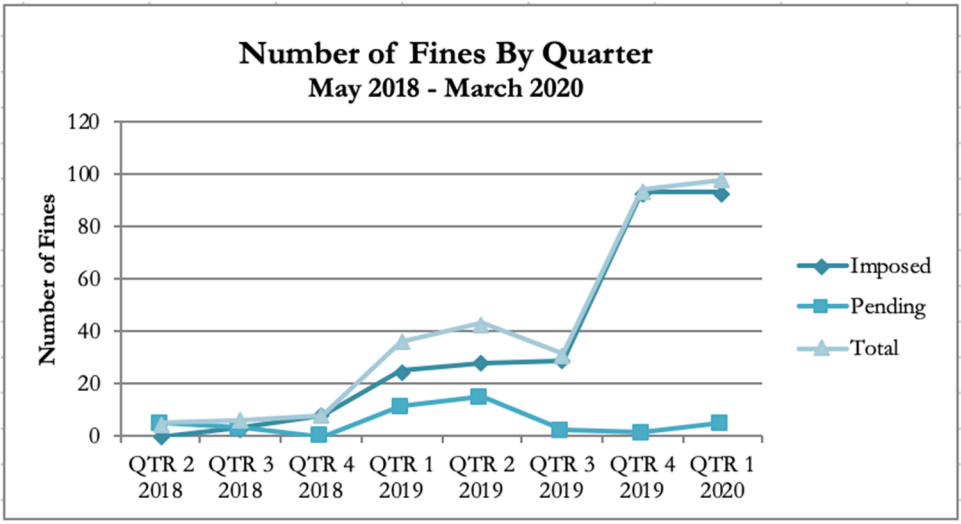
B. FINDINGS

1. Violations: Quantity and Type

The number of fines has increased steadily quarter-over-quarter and year-over-year since May 2018 with the greatest number of new fines imposed in Q4 2019. Many companies worked diligently for months to be compliant with the GDPR, in order to avoid millions of euros in penalties. In the first six months after the GDPR was enacted, fines were imposed, but in perhaps smaller numbers than expected. Imposed fines first started to increase notably in Quarter 1 of 2019. It is highly probable that DPAs started identifying targets of enforcement before May 2018, while looking for enforceable violations that took place after GDPR's enforcement date. Assuming that is the case, the initial enforcement trends suggest that it takes at least nine to ten months for a DPA to investigate and assess a fine. This timeline stands in contrast to the U.S. Federal Trade Commission, which, in non-fraud privacy cases, typically takes more than one year to investigate and assess penalties.[141] Figure 1 illustrates that the number of imposed fines increased significantly in 2019, with sixty-three new enforcement actions initiated in Quarter 4 of 2019. The leveling off of fines from the end of 2019 though the start of 2020 was likely due to lag time in the reporting of fine decisions from the end of our collection period.

141. Commenting on the FTC's relatively slow approach in 2016, Chris Hoofnagle observed, "In a single year, the FCC [Federal Communications Commission] levied $42 million in privacy fines. The FCC will soon eclipse the FTC's records of fines, which is approximately $60 million in the FTC's eighteen-year history of online privacy cases." *In* Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (Cambridge University Press 2016).

Figure 1: Number of Fines Per Quarter



Pending cases are not visibly increasing at a rate comparable to imposed fines, but it is difficult to track pending cases. Some DPA records are much more accessible and detailed than others. It is also important to note that a number of pending cases are cross-border. In these instances, multiple countries are working together to pursue enforcement actions. This requires significant cooperation and coordination, as well as record sharing. There are also some situations where one country has been designated to lead an investigation based on where the violator is established within the European Union, one example being Ireland.[142] The majority of Ireland's pending cases are directed at large U.S. technology companies whose E.U. headquarters are located in Ireland.

Fines imposed due to a violation of one or more of the seven data processing principles (Table 2) were two and a half times more frequent than fines imposed due to the violation of data subject rights (Table 3), and nearly three times more frequent than fines imposed due to a violation of controller and processor duties (Table 5). The type of violation dictates the maximum administrative fine that can be imposed. Data protection principle violations and data subject right violations (Chapters II and III in Table 5) are viewed as the most serious of all infringements, and give rise to the highest maximum

142. *See, e.g.*, Dara Murphy, *Dara Murphy: Ireland Is Up To the Data Protection Task Speech*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS DATA PROTECTION INTENSIVE (Apr. 21, 2015), https://www.youtube.com/watch?v=CMVuk0Cgg5o [hereinafter IAPP Videos].

fine allowed under the GDPR: €20 million, or four percent of a company's total worldwide annual turnover.[143]

It is interesting that data processing principle violations were a greater source of fines than data subject rights violations. Data processing principles include transparency, data minimization, and storage limitation, to name a few. Data subject rights, such as the right to data access and erasure, appear simpler to enforce than the more obscure issues of transparency and data minimization. However, DPAs can easily download companies' privacy policies and begin monitoring their compliance with the GDPR data processing principles. Individual complaints regarding data subject rights, on the other hand, probably get stuck in the review pipeline as DPAs struggle to keep pace administratively.

Table 5: GDPR Articles Cited as Reason for Violation(s)

May 25, 2018-March 31, 2020

GDPR Article Cited in Fine	Number of Citations
Chapter I – General Provisions	6
Chapter II – Principles	339
Chapter III – Rights of the Data Subject	135
Chapter IV – Controller and Processor	117
Chapter V – Transfers of Personal Data to Third Countries/Int'l Organizations	0
Chapter VI – Independent Supervisory Authorities	18
Chapter VII – Cooperation and Consistency	0
Chapter VIII – Remedies, Liability and Penalties	8
Chapter IX – Provisions Relating to Specific Processing Situations	0
Chapter X – Delegated Acts and Implementing Acts	0
Chapter XI – Final Provisions	0
Not Reported	52

A more granular breakdown of the Article 5 data processing principle violations shows that actions were most frequently brought for the infringement of the 5(a) lawfulness, fairness, and transparency principle (Figure 2). Of the 221 fines that cited a specific Article 5 violation, eighty-nine of those fines (forty percent) cited a violation of 5(a). Integrity and confidentiality and data minimization were the second and third most common principle violations, accounting for twenty-one percent and nineteen percent of Article 5 violations, respectively. Of the 135 cases that cited specific data

143. GDPR, *supra* note 21, art. 83.

subject right violations, the right to access and companies failing to provide information about the processing of information received from data subjects were the two most commonly cited infringements (Figure 3). These two violations were cited in fifty-three percent of data subject right actions where administrative fines or other nonmonetary sanction(s) were imposed or a final decision was pending.

Figure 2: Breakdown of Article 5 Data Processing Principle Violations

May 25, 2018-March 31, 2020

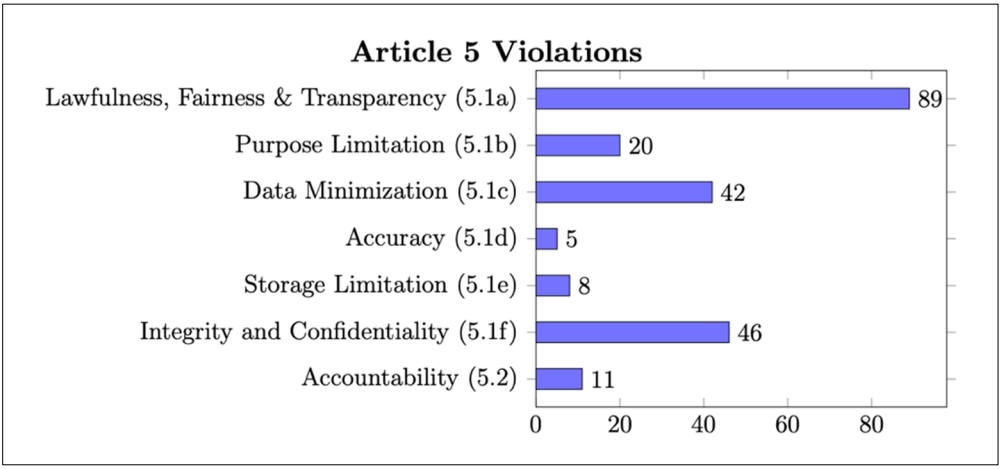
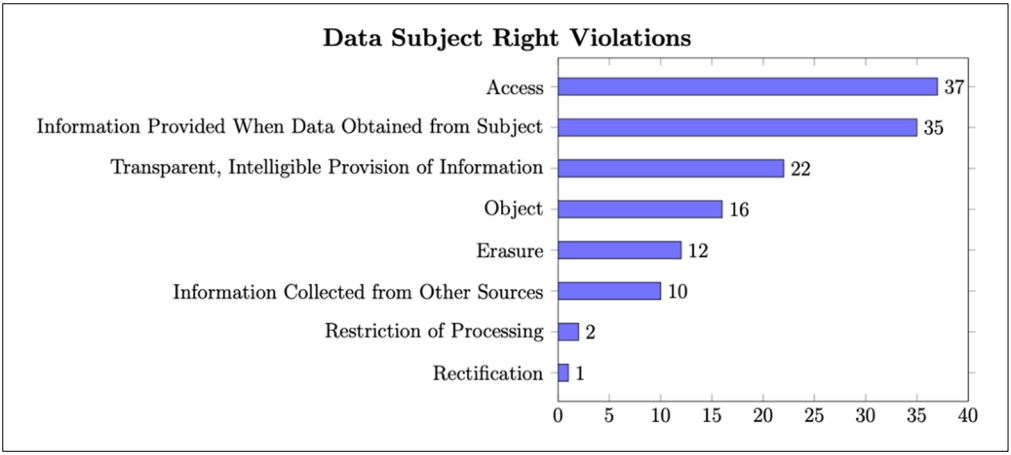


Figure 3: Breakdown of Data Subject Right Violations

May 25, 2018-March 31, 2020



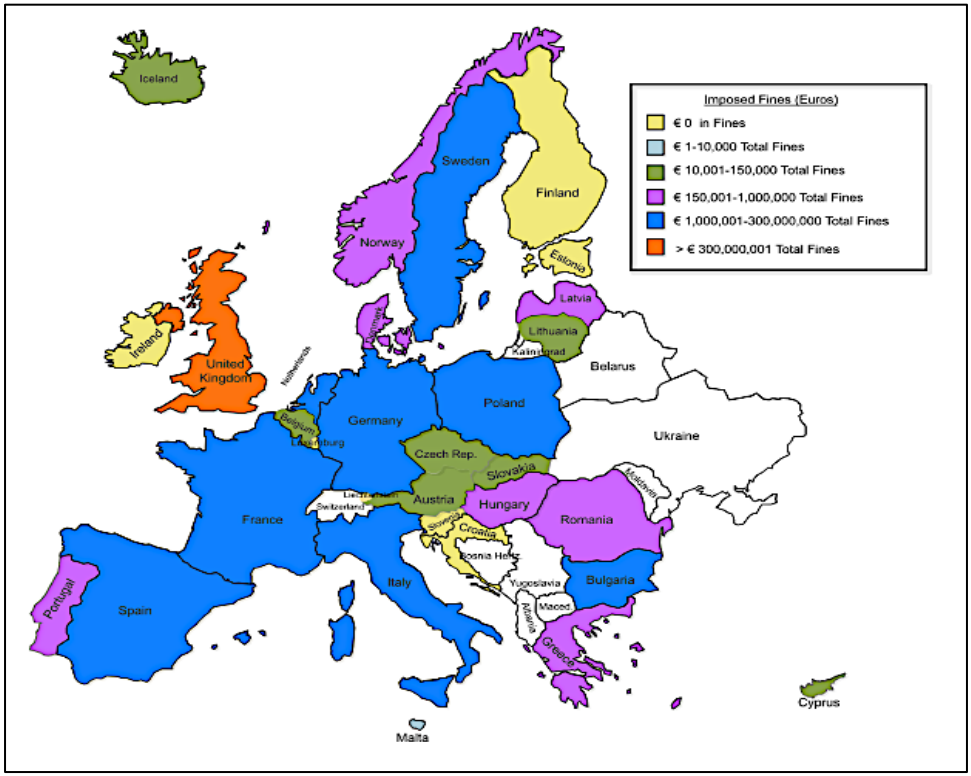
2. *Total Fines Imposed by Country*

Nine countries emerged as leaders in total fines imposed. The United Kingdom imposed €315,869,695 in GDPR fines, the highest cumulative fine total of any European country. Eight countries (Spain, France, Italy, Germany, Poland, Bulgaria, Sweden, and the Netherlands) imposed more than €1,000,001 each in total fines during the period of May 25, 2018 through March 31, 2020 (Figure 4). It could be argued that €1,000,001 in total fines over two years is actually a low total given that individual administrative fines for GDPR violations can reach €20 million, or four percent of a company's total worldwide annual turnover.[144]

A high cumulative fine total can occur from a few large fines or a number of small fines. In the case of the United Kingdom, Sweden, and the Netherlands, fines have been few but mighty. Spain, in contrast, imposed one hundred fines, more than double the total fine count of any other country.

Figure 4: Total Fines Imposed by Country

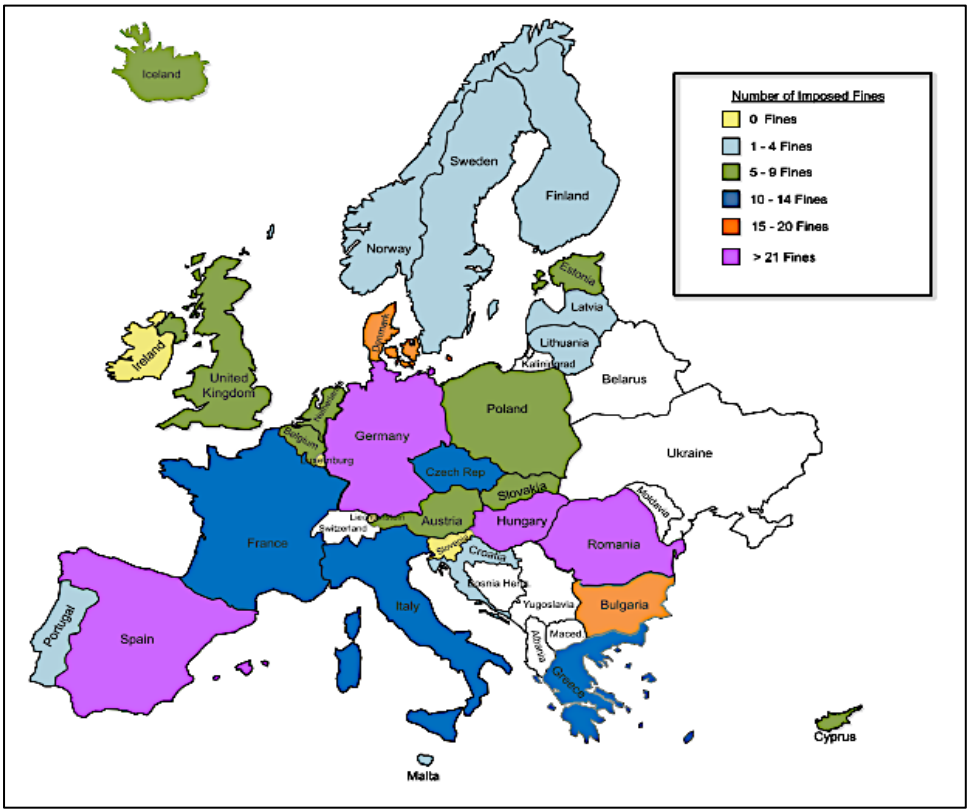
May 25, 2018-March 31, 2020



144. GDPR, *supra* note 21, art. 83.

Figure 5: Number of Imposed Fines by Country

May 25, 2018-March 31, 2020



Ireland had yet to impose any significant fines as of March 31, 2020. Ireland's Data Protection Commission (DPC) was said to be conducting as many as twenty investigations into multinational companies with highly anticipated final decisions on the horizon, but the Irish DPC did not impose its first GDPR fine until mid-May 2020, and surprisingly, it wasn't against a U.S.-based technology company.[145] This first fine was not confirmed in the Dublin Circuit Court until November 4, 2020, almost two and a half years after

145. Elizabeth Schulze, *Big Tech Fears US Regulation, But It May Be Ireland That Should Scare Them*, CNBC (June 20, 2019), https://www.cnbc.com/2019/06/20/technology-regulation-irelands-helen-dixon-has-attention-of-big-tech.html. Colm Keena, *Tulsa Becomes First Organization Fined for GDPR Rule Breach*, IRISH TIMES (May 17, 2020), https://www.irishtimes.com/news/crime-and-law/tusla-becomes-first-organisation-fined-for-gdpr-rule-breach-1.4255692.

the GDPR went into effect.[146] Ireland's actions are of great interest to many American companies who have established their E.U. headquarters there. As shown below in Table 7, as of March 31, 2020, Ireland had ten pending fines that were public, second only to Austria, the home of an active data protection advocacy organization called None of Your Business.[147] In many cross-border cases involving American technology companies, Ireland has been designated the lead supervisory authority in charge of penalty assessment because the companies' E.U. headquarters are in Ireland.[148] Because of its many pending actions, Ireland will continue to be a key country of interest. But at the same time, businesses are likely to invest heavily in defending these cases to retain Ireland's aversion to stricter continental enforcement approaches. The Irish DPC not only has many companies to oversee, it also has respondents known for scorched-earth litigation tactics. For example, Facebook (a frequent GDPR litigant), sought dismissal of one Dutch case because the court failed to adhere to the country's strict language requirements by using the words "browser" and "cookie" rather than "internetsnuffelaar" and "koekje zijn."[149]

From May 25, 2018, through March 31, 2020, there were six notably large fines, the two largest coming from the United Kingdom and followed, in order of magnitude, by France, Italy, and Germany. The majority of these fines were imposed in the second half of 2019. British Airways received the largest fine for GDPR noncompliance, resulting in a fine of 1.5% of its total revenue for the year 2018.[150] However, the United Kingdom's Information Commissioner's Office deferred the payment of the enormous fines levied against both British Airways and Marriott International twice, pending further investigations later in 2020.[151] The British Airways fine was ultimately reduced

146. *Data Protection Commission Fine on Tusla Child and Family Agency Confirmed in Court*, DATA PROTECTION COMMISSION (Nov. 4, 2020), https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-fine-tusla-child-and-family-agency-confirmed-court.

147. *See Our Detailed Concept*, NONE OF YOUR BUSINESS, https://noyb.eu/en/our-detailed-concept (last visited Mar. 31, 2020).

148. *See, e.g.*, IAPP Videos, *supra* note 142.

149. Michaël Temmerman, *With This (Strange) Argument, Facebook Strikes Back to Our Country*, HET NIEUWSBLAD (Jan. 27, 2016), https://m.nieuwsblad.be/cnt/dmf20160127_02093367.

150. Ingrid Lunden, *UK's ICO Fines British Airways a Record £183M Over GDPR Breach That Leaked Data From 500,000 Users*, TECHCRUNCH (July 8, 2019), https://techcrunch.com/2019/07/08/uks-ico-fines-british-airways-a-record-183m-over-gdpr-breach-that-leaked-data-from-500000-users/.

151. Melanie Mingas, *ICO Confirms Second Deferral For BA and Marriott's GDPR Fines*, DATA ECONOMY NEWSROOM (Apr. 17, 2020), https://data-economy.com/ico-confirms-second-deferral-for-ba-and-marriotts-gdpr-fines/.

to €20 million, a ninety-percent reduction from the initial July 2019 fine.[152] Marriott's fine was also drastically reduced to €18.4 million.[153]

Table 6: Six Largest Fines by Country[154]

May 25, 2018-March 31, 2020

Country	Date Imposed	Company	Fine Imposed (Euros)
United Kingdom	July 2019	British Airways	204,600,000
United Kingdom	July 2019	Marriot International	110,390,200
France	January 2019	Google	50,000,000
Italy	January 2020	TIM S.p.A.	27,802,946
Germany	October 2019	Deutsche Wohnen SE	14,500,000
Germany	December 2019	1&1 Telecom GmbH	9,550,000

Four of the six largest fines were imposed for insufficient security measures. The fines against British Airways, Marriott, and 1&1 Telecom GmbH were imposed for a violation of Article 32, which requires companies to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk."[155] The fine in Italy against TIM S.p.A. was also imposed, in part, due to an Article 32 violation.[156] Security vulnerabilities are generally recognized as privacy disasters because those flaws can be exploited by "hackers" and other malicious actors. Once data are stolen, all use-based and policy-based controls on it are impossible to enforce. In some cases, these data end up on publicly-available websites for anyone to download. This represents a total failure of market promises of security. Insufficient security measures will thus likely continue to be a catalyst for high fines because the harm is evident and company expectations under the GDPR

152. *ICO Fines British Airways £20m for Data Breach Affecting More Than 400,000 Customers*, INFORMATION COMMISSIONER'S OFFICE (Oct. 16, 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/.

153. *ICO fines Marriott International Inc £18.4million For Failing to Keep Customers' Personal Data Secure*, INFORMATION COMMISSIONER'S OFFICE (Oct. 30, 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/.

154. Both U.K. fines were significantly reduced by the ICO in October 2020.

155. GDPR, *supra* note 21, art. 32(1).

156. *Marketing: From the Privacy Guarantor a Fine of 27 Million and 800 Thousand Euros to Tim*, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (Feb. 1, 2020), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256409.

are clear—companies are obligated to implement procedures that appropriately protect consumers' personal data. In contrast, other privacy violations are more challenging to assess given that many of the GDPR articles are written at principle-level abstraction.

3. Comparing Total Fines by Country to Gross Domestic Product

When comparing each country's gross domestic product (GDP) against the total number of fines each country imposed, countries with high GDPs imposed more fines and higher fines than countries with lower GDPs. GDP is a monetary measure of the market value of total goods and services produced by a country, and is considered a powerful indicator of economic development and progress. With the exception of Ireland, the three countries that had yet to impose a fine under the GDPR as of March 31, 2020, had a thirty-third percentile GDP when compared to the GDP of the thirty-one countries subject to the GPDR. The top nineteen countries by GDP (again excluding Ireland) had all imposed some number of fines. There were three countries in the fifty-fifth percentile by GDP that imposed a number of fines: Romania, Hungary, and Bulgaria (Table 7). In Table 4 above, we categorized each of these countries in our March 2020 assessment as having a "progressing" approach towards GDPR enforcement. Nearly all of the fines, in each of these three countries, were imposed in 2019 and 2020. This suggests that countries with less economic resources took slightly longer to mobilize, but fines are now on the rise in these countries as well.

In Table 4 above, we categorized five countries in our March 2020 analysis as having a "vigorous" approach to GDPR enforcement: France, Germany, Italy, Spain, and the United Kingdom. In 2019, these countries were the top five GDP earners across the European Union. It is not surprising that countries with strong economies would have the resources to create a robust GDPR enforcement infrastructure. Specific countries, such as Germany and the United Kingdom, arguably took the lead on enforcement actions, while other countries may be waiting for more precedent and cooperation standards to be set by these leaders. The ombudsman of Finland, one of the countries categorized as "cautious," has publicly spoken about the importance of E.U. harmonization, and it is expected that the European Data Protection Board guidelines will strongly influence Finland's future GDPR enforcement.[157] This is one example of how some countries, even those with a sizeable GDP, are taking a more cautious approach to enforcement, waiting to see how guidelines and cooperation mechanisms develop across the EU.

157. IUS LABORIS, *supra* note 115.

Additionally, there is a positive correlation between fine amount and the GDP of the country where the fine is issued. GDPR violators pay higher fines in countries with higher GDPs. As GDP increases by €1 million, the fine amount increases by €2,770.[158]

158. This is based on a regression of 268 enforcement cases at a ninety-nine-percent confidence level with an R-squared value of 0.032.

Table 7: 2019 Gross Domestic Product[159] and Fines by Country[160] (Count & Monetary Value)

Country	2019 Annual GDP (Euro-Millions)	Imposed Fines (Euros)	Implemented Fines /Sanctions (Count)	Pending Fines /Sanctions (Count)	Total Imposed and Pending Fines/Sanctions (Count)
Germany	3,435,990	25,060,925	21	4	25
United Kingdom	2,523,314	315,869,695	6	1	7
France	2,418,997	52,050,000	12	2	14
Italy	1,787,664	39,454,946	11	1	12
Spain	1,244,757	2,501,270	100	0	100
Netherlands	812,051	2,535,000	6	3	9
Poland	527,033	1,047,248	8	1	9
Sweden	474,683	7,053,630	3	1	4
Belgium	473,639	39,000	6	3	9
Austria	398,522	70,200	7	11	18
Norway	359,109	400,400	4	4	8
Ireland	347,215	0	0	10	10
Denmark	310,576	381,850	17	0	17
Finland	240,924	0	2	1	3
Romania	222,090	495,500	25	0	25
Czech Republic	219,896	19,035	11	2	13
Portugal	212,303	422,000	3	0	3
Greece	187,457	750,000	13	1	14
Hungary	143,826	218,183	24	0	24
Slovakia	94,177	90,000	6	0	6
Luxembourg	63,516	0	0	0	0
Bulgaria	60,675	2,744,820	17	1	18
Croatia	53,937	0	1	0	1
Lithuania	48,339	61,500	1	0	1
Slovenia	48,007	0	0	2	2
Latvia	30,476	157,000	2	0	2
Estonia	28,037	0	8	1	9
Cyprus	21,944	121,000	8	0	8
Iceland	21,603	29,000	5	0	5
Malta	13,209	5,000	1	0	1
Liechtenstein*	5,823	0	0	0	0
	Totals	**451,577,202**	**328**	**49**	**377**

* 2018 GDP in Euro-Millions

159. *GDP—Gross Domestic Product*, COUNTRYECONOMY.COM, https://countryeconomy.com/gdp (last visited Aug. 6, 2021).

160. This table includes forty-one implemented nonmonetary sanctions and one pending nonmonetary sanction.

4. Fines by Economic Sector

One goal of the GDPR was to update data protection law so E.U. citizens would be adequately protected in an era of constant technological innovation; the size and quantity of fines imposed against technology companies in the first two years of implementation are consistent with that objective. Economists view the economy as divided into four main sectors: primary, secondary, tertiary, and quaternary. A "sector" is a subset of businesses that share similar product or service offerings, as described in Table 8. Interestingly, the tertiary economic sector, which encompasses companies that provide enterprise and consumer services, received the most fines. The quaternary sector, the sector that includes technology companies, received significantly fewer fines. However, the quaternary sector did receive some of the largest fines imposed under the GDPR and had the most fines pending of any sector.

Perhaps surprisingly, multiple small fines totaling just a few hundred euros were imposed, and primarily against companies in the tertiary sector (enterprise and consumer services). A €300 fine was charged to a private car owner in Austria for inappropriate use of Dashcam, a camera that records a vehicle's travel through the front and sometimes rear windshields. The Czech Republic imposed a €388 fine against an employer that did not properly delete data on its Facebook page about a former employee.

A variety of industries have received fines, such as schools, taxi companies, restaurants, banks, political campaigns, and even private persons. For example, a school in Sweden was fined €18,630 for inappropriately using facial recognition to monitor student attendance. Simply put, no industry or individual is immune to GDPR enforcement.

Table 8: Imposed and Pending Fines and Nonmonetary Sanctions by Economic Sector[161]

May 25, 2018-March 31, 2020

Economic Sectors	Description	Imposed Fines	Pending Fines
Primary	Extraction and harvesting of natural resources such as agriculture and mining.	0	0
Secondary	Comprises construction, manufacturing, and processing. Basically, this sector comprises industries that relate to the production of finished goods from raw materials.	2	0
Tertiary	This type of industry provides services and includes companies such as retailers, entertainment, financial, insurance, social and personal services. These companies provide services to consumers and business.	245	5
Quaternary	This sector deals with knowledge or intellectual pursuits including research and development, business, consulting services, and education.	30	43

U.S. companies were not disproportionately fined overall, but U.S. technology companies did receive the majority of quaternary sector fines. Of the 325 fines (imposed and pending) where an economic sector could be identified, only forty-eight actions (eight imposed, forty pending) were against U.S. companies. However, the majority of those forty-eight U.S. actions were against U.S. "big tech" companies. A total of thirty-eight of the forty-eight U.S. actions (seventy-nine percent) involved "big tech" players: Apple, Amazon, Facebook, Google, Microsoft, Twitter, and Uber. European DPAs are fining many more tertiary sector companies than quaternary sector companies, but of the seventy-three actions taken against companies in the quaternary sector (thirty imposed fines, forty-three pending), forty-four of them (sixty percent) were against U.S. technology companies. Additionally, one of the six largest fines imposed during the first two years of GDPR enforcement was against a large U.S. tech company (Google). The five other largest fines were imposed against service industry companies, including the U.S. hotel chain Marriott. Within the quaternary sector, European DPAs are disproportionately fining U.S. technology companies, and the fines they impose are significant. The

161. For fifty-two fines, a company name and/or industry could not be identified.

lowest fine received by a U.S. technology company was a 2019 fine of €51,000, more than four times the 2019 fine median, €11,380.

AdTech, short for advertising technology, is a booming field that is a specific target of the GDPR.[162] AdTech is a term used to describe the software and tools that companies use to send targeted online advertisements to potential customers. In January 2019, France fined Google €50 million for failing to fully explain its personalized advertising data collection process during the Android phone set-up process.[163] France's DPA, the Commission Nationale de l'Informatique des Libertés (CNIL), charged Google with not being transparent enough in its explanations regarding data collection and use for advertising purposes.[164] During its investigation, the CNIL observed that relevant information about advertisement personalization was disseminated across several documents during the Google account creation process, and the "Ads Personalization" section did not adequately explain to users the multitude of company services and applications involved in the process (e.g., Google search, YouTube, Google Maps, etc.).[165] Advertising technology is complicated and data is used to serve ads in ways that are not always straightforward or easy to explain to a layperson.[166] Moreover, Google is a huge company with vast legal resources. If its legal team can't satisfy France's transparency and consent requirements, smaller companies are surely in trouble if France continues to uphold these interpretations.

France's fine against Google is a case where the findings matter, not the fine. If the CNIL's interpretation of transparency is adopted by other countries, Google might be prohibited from doing the targeted advertising it wants to do because it will be impossible to keep the process transparent. As sophisticated neural networks are increasingly being used to target ads through machine learning, it might not be possible to explain in a human readable format why one profiled data subject receives a certain advertisement while

162. GDPR, *supra* note 21, art. 3(2). Under Article 3(2), "monitoring" Europeans' behavior—even without maintaining a European presence—is a regulated activity under the GDPR.

163. *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC*, CNIL (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

164. *Id.*

165. *Id.*

166. Taylor Wessing, *Adtech—What Do the EU Regulators Think?*, LEXOLOGY (Sept. 8, 2019), https://www.lexology.com/library/detail.aspx?g=6048f2da-ffce-4c44-8225-d0e4027cb0a6.

another data subject does not.[167] The CNIL's rationale threatens the viability of using complex machine learning systems to improve advertising.

V. ANTICIPATED GDPR ENFORCEMENT TRENDS

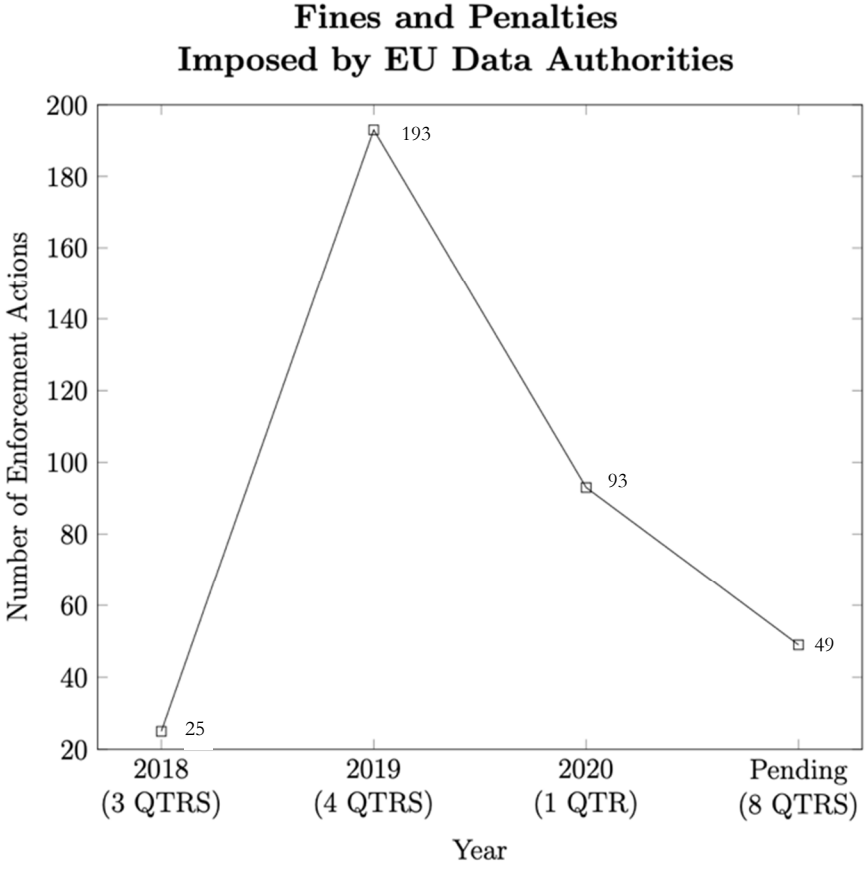
The upward trend in fines will likely continue. The number of fines imposed (Figure 6) increased nearly eightfold from 2018 (twenty-five fines) to 2019 (193 fines); ninety-three fines were imposed in the first quarter of 2020 alone. Factors that may have greatly impacted fine variability across the European Union—lack of resources, country implementation approach, and national privacy legislation timeline—will have a lesser impact on individual member state enforcement actions with time.

Even though, with time, E.U. member states have become better equipped to enforce the GDPR, there are still a number of factors which affect fine assessment that will continue to evolve and change country-by-country such as political climate, cultural and economic priorities, and industry presence. Even with more resources and improved collaboration methods, complete harmonization of administrative fine practices across all E.U. member states seems unlikely. Country DPAs, like any regulatory authority, set priorities based on the opinions of its internal decision makers and the feedback provided by its constituents. Even with knowledge sharing mechanisms and the EDPB advisory board dedicated to issuing GDPR implementation guidance, individual countries will surely have differing visions regarding on-the-ground enforcement. The question, then, is which metrics, if any, can appropriately evaluate the success of the GDPR? What does success look like in the context of this complex, wide-reaching regulation?

167. *See generally* Walter A. Mostowy, Note, *Explaining Opaque AI Decisions: How to Satisfy the GDPR's Right to an Ex Post Explanation*, 35 BERKELEY TECH. L.J. 1291 (2020).

Figure 6: Total Fines and Nonmonetary Sanctions Imposed and Pending[168]

May 25, 2018-March 31, 2020



A lot of progress has been made regarding the preparatory work needed to diligently oversee companies' data processing practices, including passing legislation, restructuring agencies, and allocating funding and resources, something many countries initially lacked. Countries like Germany, with a longstanding history of prioritizing privacy and DPAs already equipped with resources and established operational processes, were better prepared to support the changes being made under the GDPR. Other countries were required to restructure their agencies and have struggled to keep up with the increase in data breach notices and complaint submissions. Belgium's Data Protection Authority, for example, was not fully operational until April 25,

168. The graph only includes fines and nonmonetary sanctions with publicly available dates.

2019, almost a full year after the GDPR was enacted.[169] Many countries that needed time to restructure their regulatory bodies, adopt national privacy legislation, and adapt to the new data protection landscape under the GDPR are now, three years later, better equipped to enforce penalties for noncompliance. The work is flooding in: DPAs received over 281,088 cases during the first year of GDPR enforcement.[170] However, enforcement is still challenging for many national DPAs. Some member states voiced concerns about the administrative burden being placed on DPAs and companies under the Regulation.[171]

Harmonization, one of the key tenants of the GDPR, is in some ways taking root. A number of countries have found ways to be innovative in their approach to GPDR implementation. Austria and Hungry both took the approach of issuing warnings for first infringements. Many countries prioritized educating companies and thus spent time drafting GDPR guidelines and best practices, only issuing fines when companies refused to cooperate. Numerous countries, in adopting new national privacy laws, implemented country-specific derogations unique to their national security, economic, and financial interests. All of these micro-decisions by different countries made harmonization and cross-border cooperation more challenging. But with the GDPR in effect for three years now, the implementation grace period is running out. Some countries are starting to take the lead on harmonization efforts. Germany developed a five-step fining structure to ensure that administrative fines are issued in an accurate and consistent manner.[172] While the German fine model is complex and not without critics, the European Data Protection Board (an independent body in charge of GDPR implementation) could conceivably create a similar standardized fine model that would be binding across the European Union. Furthermore, nineteen countries released their perspectives on GDPR in

169. Laura Brodahl, Laura De Boel, Jan Dhont & Cédric Burton, *Belgian Data Protection Authority Is Up and Running*, WILSON SONSINI (Apr. 26, 2019), https://www.wsgrdataadvisor.com/2019/04/belgian-dpa/.

170. Case total based on information provided by twenty-seven countries. *1 Year GDPR—Taking Stock*, EUROPEAN DATA PROTECTION BOARD (May 22, 2019), https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en.

171. Preparation of the Council Position on the Evaluation and Review of the General Data Protection Regulation (GDPR) - Comments from Member States, COUNCIL OF THE EUROPEAN UNION (Oct. 9, 2019), https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf.

172. Tim Wybitul, *German DPAs Push Model for Higher GDPR Fines*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Oct. 1, 2019), https://iapp.org/news/a/german-dpas-push-model-for-higher-gdpr-fines/.

practice prior to the E.U. Council's formal evaluation of the GDPR,[173] which was released on January 15, 2020.[174] The European Commission also released an evaluation and review of the first two years of GDPR enforcement.[175] Time will provide opportunities to review the successes and challenges of the GDPR across the European Union, informing and improving harmonization efforts going forward.

Yet certain immeasurable factors that data cannot track—specifically a country's political climate—may be the most indicative of the future GDPR challenges the European Union could face. Fines are not imposed in vacuums; they are imposed by real people with existing loyalties and motivations. Although France sent a strong message to the AdTech industry when it fined Google heavily for not clearly explaining its online advertising practices, it also closed three cases against small French AdTech firms with only a request that the firms update their customer consent collection methods.[176] Ireland has been the hotspot for pending litigation against large U.S. technology companies, but the country abstained from issuing a single fine for two years.[177] As a final example of politics in action, the United Kingdom was engulfed in Brexit turmoil even before the GDPR became enforceable. In January 2020, the United Kingdom formally withdrew from the European Union.[178] Uncertain as to whether it was going to remain an E.U. member state, it is possible that the United Kingdom issued large fines partially to send a message that its data protection standards are high and deserving of an adequacy decision as a sovereign nation. Interestingly, two of the largest fines imposed by the United Kingdom Information Commissioner's Office were ultimately reduced significantly at the end of 2020 despite the fact that the European

173. Müge Fazlioglu, *GDPR in the Eyes of the Member States*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Oct. 16, 2019), https://iapp.org/news/a/gdpr-in-the-eyes-of-the-member-states.

174. *Council Position and Findings on the Application of the General Data Protection Regulation (GDPR)—Adoption*, COUNCIL OF THE EUROPEAN UNION (Jan. 15, 2020), https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/en/pdf.

175. Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition—Two Years of Application of the General Data Protection Regulation, EUROPEAN COMMISSION (June 24, 2020), https://ec.eropa.eu/info/sites/info/files/1_en_act_ part1_ v6_1.pdf.

176. What the CNIL's Recent Decisions Involving Vectaury, Fidzup, Teemo and Singlespot Reveal About What a Consent UI Should Look Like, ONETRUST (Dec. 14, 2018), https://www.onetrust.com/cnil-vectuary-fidzup-teemo-singlespot-what-it-means/#.

177. Colm Keena, *Tulsa Becomes First Organization Fined for GDPR Rule Breach*, THE IRISH TIMES (May 17, 2020), https://www.irishtimes.com/news/crime-and-law/tusla-becomes-first-organisation-fined-for-gdpr-rule-breach-1.4255692.

178. *See generally Brexit: All You Need to Know About the UK Leaving the EU*, BBC (Feb. 17, 2020), https://www.bbc.com/news/uk-politics-32810887.

Commission is still finalizing the United Kingdom's adequacy request.[179] In the interim, data flows between the United Kingdom and European Union can continue until June 30, 2021, pursuant to the E.U.-U.K. Trade and Cooperation Agreement.[180] The above examples expose some of the intangible truths behind the data, and their importance should not be overlooked. No matter how standardized the European Union tries to make data protection processes, E.U. member states will continue to have their own values, motivations and challenges that will undoubtedly affect their individual approaches to GDPR enforcement.

VI. CONCLUSION

The number of administrative fines imposed increased almost eightfold from 2018 to 2019, and ninety-three fines were imposed in the first quarter of 2020 alone. Some types of infringements resulted in more fines than others. It may be because those violations are broadly defined, as is the case with the "lawful, fair, and transparent" data processing principle, or the violations are particularly obvious to the user, as is true of the data subject's right to "access" his or her data. Certain countries continue to lead the charge with enforcement, like Germany and France. Their high GDPs and strong history of privacy protection resulted in a vigorous implementation approach that was not hindered by a lack of resources or infrastructure. The technology sector was issued a number of fines, and they were sizeable, but there were also a substantial number of "little guys," like schools, political campaigns, restaurants, and private individuals fined for noncompliance.

The GDPR is a massive regulation that requires time to implement. The European Union is striving for the GDPR in its entirety, and specifically the administrative fines, to be implemented in a consistent manner across all twenty-seven E.U. member states and three EEA countries. Each iteration of E.U. privacy legislation has pushed for improved harmonization in data protection practices across the European Union. The Article 29 Data Protection Working Party suggested that DPAs have regular exchanges including "case-handling workshops or other events" to allow countries to compare their treatment of cases and resulting fines and corrective measures.[181]

179. *See* European Union, *Adequacy Decisions*, OFFICIAL WEBSITE OF THE EUROPEAN UNION, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Apr. 23, 2021).

180. European Union, *Data protection: European Commission launches process on personal data flows to UK*, OFFICIAL WEBSITE OF THE EUROPEAN UNION, https://ec.europa.eu/commission/prescorner/detail/en/ip_21_661 (last visited Apr. 23, 2021).

181. Article 29 Data Protection Working Party, *supra* note 16, at 17.

It will take time for E.U. member states to establish these collaborative methods and channels of communication and build out the resources necessary for member states to work together efficiently.

Early obstacles to harmonization—lack of resources, country-specific implementation approaches, and national privacy legislation timelines—will have less impact on enforcement actions over time. For example, it is difficult for a country to actively enforce the GDPR when it is still deciding which derogations to implement. Once national legislation is passed, DPAs will have the ability to fully enforce the GDPR and work through issues that arise. Cross-border cooperation will also improve and case law will develop, both becoming tools for more consistent decision making. Despite anticipated short-term improvements in harmonization, variability in approaches to GDPR enforcement will remain a long-term challenge due to member states' differing cultural, philosophical, and political opinions on implementation.

The GDPR has had a global impact. Countries around the world (most recently South Korea and the United Kingdom) are seeking adequacy decisions from the European Commission.[182] There have also been discussions about the recently passed California Privacy Rights Act (CPRA) and whether the individual state of California could be eligible for adequacy. With an adequacy decision, personal data can flow between the "adequate" country and all E.U. member states (as well as the three EEA countries subject to the GDPR), without the use of additional data transfer safeguards.[183] One of the most watched conversations in 2021 will be the renegotiation of the E.U.-U.S. Privacy Shield, a framework for allowing data exchanges between the United States and the European Union, after the Court of Justice of the European Union invalidated the existing agreement in July 2020.[184] Additionally, the COVID-19 pandemic has brought to light many international privacy practices as countries attempt to monitor sick patients and enforce quarantine practices to slow the viral spread. Sensitive health information has never been more top of mind, and the balance between personal privacy and public safety is

182. OFFICIAL WEBSITE OF THE EUROPEAN UNION, *supra* note 179; European Union, Slides—Internal EU27 Preparatory Discussions on the Future Relationship: "Personal Data Protection (Adequacy Decisions), Cooperation and Equivalence in Financial Services", OFFICIAL WEBSITE OF THE EUROPEAN UNION, https://ec.europa.eu/commission/sites/beta-political/files/seminar_20200110_-_data_protection_adequacy_-_financial_services_en.pdf (last visited Apr. 12, 2020).

183. OFFICIAL WEBSITE OF THE EUROPEAN UNION, *supra* note 179.

184. *See* C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems*, COURT OF JUSTICE OF THE EUROPEAN UNION (July 16, 2020), http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en.

precarious. As privacy laws continue to develop and evolve around the globe, there will be many more voices offering input regarding the interpretation and operationalization of E.U. data protections standards.

Fines have been a huge focus since the GDPR became law, but the success of the GDPR is not just defined by fines—the most important question is how the GDPR shapes the future of data privacy. Are administrative fines substantively enforced, or are they merely punitive penalties with little impact on companies' actual behavior? Certain countries, particularly Germany and France, have aggressively imposed fines and taken actions to solidify what is means to "comply" with different provisions of the Regulation. Ireland, comparatively, is the European hub for many large technology companies whose practices are hotly contested, but it has done little to direct the behavior of those companies. If Ireland were to impede the actions of those companies, its economy could be negatively impacted, thus at least partially explaining its inaction. Many of these large technology companies also have deep pockets and are willing to endure expensive litigation. But if some countries are much easier for businesses to operate in than others, businesses will flock to the countries where their operations are least impacted. That could have a ratcheting effect on harmonization, possibly causing countries who are substantively strong on enforcement to suffer economically. Most businesses would prefer to pay a fine and retain the ability to use personal data how they wish over an order to implement restrictive, costly practices. The E.U. member state divide between punitive and substantive enforcement has already begun, and we predict it will continue to grow.

This Note has framed the processing of personal data as a focus of regulation, but the GDPR exists in a larger, complex, growing regulatory environment. All indications point to a desire to impose more rules on companies, especially high technology companies. The European Union's Digital Services Act, aimed at improving safety on digital platforms, is in progress.[185] The goal of the European Union's new ePrivacy Regulation is to safeguard the privacy of electronic communications.[186] The European Commission recently released proposals for an Artificial Intelligence Regulation and a complementary Machinery Regulation, outlining health and

185. European Union, *The Digital Services Act: Ensuring a Safe and Accountable Online Environment*, OFFICIAL WEBSITE OF THE EUROPEAN UNION, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en#what-are-the-next-steps (last visited Apr. 23, 2021).

186. Müge Fazlioglu, *Next-gen privacy: Examining the EU's ePrivacy Regulation*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Feb. 17, 2021), https://iapp.org/news/a/nextgen-privacy-the-eus-eprivacy-regulation/.

safety requirements for a wide range of machinery products.[187] These are just three examples of GDPR adjacent legislation that work to limit the freedom of technology companies. In many ways, the GDPR accelerated these other regulatory regimes because it forced companies to be more transparent about how they use customers' personal information, exposing the widespread existence of objectionable business practices. We could move from a world where technological innovation drives progress and policy to one where each technology product or service has specified rules and requirements, with no way to circumvent those specifications. Small companies are already disproportionately burdened by GDPR compliance requirements. Furthermore, consent-based privacy models like the GDPR are difficult to apply to emerging technologies like artificial intelligence, machine learning, and facial recognition. The very regulations Europe is creating to protect its citizens could have the unintended consequence of stifling the growth and creativity of the technology sector. The durability and adaptability of the GDPR will be an important benchmark as we continue to make decisions that shape the future of data privacy.

187. European Union, *Europe Fit for the Digital Age: Commission Proposes New Rules and Actions for Excellence and Trust in Artificial Intelligence*, OFFICIAL WEBSITE OF THE EUROPEAN UNION, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 (last visited Apr. 23, 2021).