Harvard Journal of Law & Technology Digest
Online-only publication

Innovating in Uncertainty: Effective Compliance and the GDPR

Filippo A. Raso[*]

Published August 14, 2018
Original link: https://jolt.law.harvard.edu/digest/innovating-in-uncertainty-effective-compliance-and-the-gdpr

Recommended Citation

Filippo A. Raso, Note, *Innovating in Uncertainty: Effective Compliance and the GDPR*, Harv. J.L. & Tech. Dig. (2018), https://jolt.law.harvard.edu/digest/innovating-in-uncertainty-effective-compliance-and-the-gdpr.

[*] J.D., Harvard Law School, Class of 2018; H.B.Sc., University of Toronto Scarborough, Class of 2014. This Note, in a substantially similar form, earned a special mention in the William & Mary Law School Artificial Intelligence Legal Issues International Paper Competition. Thank you to John DeLong for teaching an exceptional class leading to this Note and to Phillip Takhar at Harvard's Journal of Law and Technology Digest for his patience and diligence.

Table of Contents

I. Introduction

The global regulatory landscape for data protection lurched into new territory on May 25, 2018: the day the European Union's General Data Protection Regulation ("GDPR" or "Regulation") came into force.[1] Much has been said about the GDPR's paradigmatic shift in data protection rules, including how the Regulation will impact data-driven innovations such as machine learning, Big Data, or artificial intelligence. Some commentators assert that the GDPR prohibits such analysis;[2] others argue they will flourish with renewed vigor.[3] These debates are indicative of the uncertainty surrounding the GDPR regime. How strictly will the Regulation be enforced? Which interpretations of the many provisions and exceptions will come to predominate regulatory enforcement? Even still, what derogations will implicate these technologies? Indeed, the regulatory waters ahead are murky.

[1] Regulation (EU) 2016/679 of the European Parliament and 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), 2016 O.J. L 119/1 [hereinafter GDPR].

[2] *See, e.g.*, Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 Seton Hall L. Rev. 995 (2017).

[3] *See, e.g.*, Viktor Mayer-Schönberger & Yann Padova, *Regime Change? Enabling Big Data Through Europe's Data Protection Regulation*, 17 Colum. Sci. & Tech. L. Rev. 315 (2016).

Yet the GDPR commands immediate obedience; malfeasance will be met with stiff penalties. Thus, the challenge facing those employing data-driven analytics becomes obvious. What it means for them to "obey" the GDPR is far from clear. One reading of the GDPR outlaws these technologies; the other promotes them. For better or worse, the regulatory landscape will continue to shift under their feet as enforcement and judicial review refines, limits, and makes sense of the behemoth Regulation. At the same time, these companies must continue to collect, analyze, and act on data. Failing to do so is a threat to their very survival and to the technological capacity of Europe. Simply put, how do data-driven companies continue to innovate while facing the threat of exorbitant fines?

This Note offers a simple answer: an effective compliance program. As explained below, the GDPR calls for mitigating damages against companies who undertake good-faith efforts to adhere to the law. Such efforts will invariably entail the design, implementation, and enforcement of strong corporate policies and procedures—internal controls—to comply with the Regulation. To guide the development of these internal controls, companies and their counsel should look to existing guidelines on effective compliance programs, such as those promulgated by the United States Federal Sentencing Guidelines for Corporations ("Sentencing Guidelines").

This Note begins by briefly summarizing the literature about the GDPR and data-driven analytics in Part II, with a focus on specific GDPR provisions. Drawing on the Regulation's text and commentary from leading officials, Part III argues the GDPR embraces effective compliance programs as a significant mitigating factor in levying penalties. To provide more clarity to what constitutes an "effective" program, this Part looks to the Sentencing Guidelines. Lastly, Part IV assesses, in broad strokes, what the seven elements of the Sentencing Guidelines might demand of a controller employing advanced data analytics under the GDPR.

II. The GDPR and Data-Driven Analytics

A heated debate has developed seeking to answer the following question: does the GDPR prevent or unreasonably inhibit Big Data, artificial intelligence, and the like? No consensus yet exists.[4] While clear that the Regulation applies to these technologies, questions remain about whether strict compliance ultimately defeats their purpose. This Part briefly summarizes key GDPR provisions and their position in the ongoing argument. The provisions discussed are Article 5(1)(b) (purpose limitation),[5] Article 5(1)(c) (data minimization),[6], and Article 22 (limiting automated decision-making).[7]

Article 5 sets out the Principles data controllers must follow when processing personal data.[8] One such principle is purpose limitation.[9] Purpose limitation obliges controllers to collect data only for "specified, explicit and legitimate purposes" and prohibits further processing of collected data "in a manner that is incompatible with those purposes."[10] Several notable exceptions allow further processing.[11] Critics have charged

[4] *See supra* notes 2-3 and accompanying text.

[5] GDPR, art. 5(1)(b).

[6] GDPR, art. 5(1)(c).

[7] GDPR, art. 22. Other rights and obligations implicate data-driven analytics like machine learning, such as the GDPR's elevation of special categories of data, the right to explanation, and the right to be forgotten. For a discussion of the right to be forgotten, see Wei Chieh Lim, *Will Data Protection Laws Kill Artificial Intelligence?*, CPO Mag. (Aug. 17, 2017), https://www.cpomagazine.com/2017/08/17/will-data-protection-laws-kill-artificial-intelligence/2/.

[8] GDPR, art. 5. Personal data is defined as "any information relating to an identified or identifiable natural person[, which] is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR, art. 4(1). Data controllers are those who "determine[] the purposes and means of the processing of personal data." GDPR, art. 4(7).

[9] GDPR, art. 5(1)(b).

[10] GDPR, art. 5(1)(b).

[11] *See* GDPR, art. 5(1)(b) ("[F]urther processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes."). Article 89(1) states further processing "shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place." However, Recital 162 states statistical analysis cannot be "used in support of measures or decisions regarding any particular natural person." Even though recitals are not binding, they call into question whether using machine learning algorithms fall within the "statistical purposes" exception.

the Principle of purpose limitations as being antithetical to data-driven analytics; it diminishes economic value and prevents innovation.[12]

These criticisms are made in light of the belief in the "four Vs" of big data and artificial intelligence: "the Volume of data collected, the Variety of sources, the Velocity [of] the analysis . . . and the Veracity of the data."[13] Perhaps unsurprisingly, regulators have routinely disagreed with that assessment. Interpreting the same language under the Data Protection Directive, the Article 29 Data Protection Working Party[14] observed "the legislators intended to give some flexibility with regard to further use. Such further use may fit closely with the initial purpose or be different."[15] Moreover, the GDPR presumes that statistical or research purposes are to be "compatible" uses.[16] The United Kingdom's Information Commissioner's Office says that future processing is permissible so long as "it is fair."[17] Their argument, essentially, is that the GDPR explicitly permits the future processing of data for statistical and research purposes.

Article 5 further sets out a data minimization requirement.[18] Data minimization demands personal data be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."[19] Here, concerns focus on the essence of data-driven analytics: extracting unseen patterns from large data sets.[20] Data-driven analytics function by simultaneously evaluating myriad variables, including those seemingly irrelevant, to uncover the hidden insight. Indeed, if the "nec-

[12] *See, e.g.*, Unlocking the Value of Personal Data: From Collection to Usage, World Econ. Forum 7 (Feb. 2013), http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf; *see also* Zarsky, *supra* note 2, at 1005.

[13] Zarsky, *supra* note 2, at 998-99.

[14] The Article 29 Data Protection Working Party was an advisory board launched in 1996 pursuant to article 29 of the Data Protection Directive. Its responsibilities included, among many others, offering persuasive interpretations of the Directive. The GDPR replaced the Working Party with the European Data Protection Board, which adopted the Working Party's opinions.

[15] Opinion 03/2013 on Purpose Limitation, Article 29 Data Protection Working Party 21 (Apr. 2, 2013).

[16] Principle (b): Purpose Limitation, U.K. Info Commc'ns Office, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (last accessed July 5, 2018).

[17] Big Data, Artificial Intelligence, Machine Learning and Data Protection, U.K. Info Commc'ns Office 38 (Sept. 4, 2017).

[18] GDPR, art. 5(1)(c).

[19] GDPR, art. 5(1)(c).

[20] Zarsky, *supra* note 2, at 1010-11.

essary" data points were already known, these technologies would not offer such groundbreaking insights.[21] Proponents of the Regulation argue, in turn, that the Principle does not prevent companies from collecting lots of data; it only prevents them from collecting irrelevant and unnecessary personal data.[22] Moreover, companies adopting other technical approaches to anonymize data can escape these obligations.

Most relevant to artificial intelligence technologies is Article 22: limits on automated decision-making.[23] Article 22 grants data subjects rights to avoid automated decision-making that has legal or other significant effects.[24] The Article 29 Working Party explains that this prohibition is meant for "only serious impactful events" such as "denial of a particular social benefit granted by law . . . refused admission to a country . . . automatic refusal of an online credit application . . . [and] significantly affect[ing] the circumstances, behavior, or choice of the individuals involved."[25] Despite including several exceptions, Article 22 is lamented as a "rejection of the Big Data revolution" because its exceptions require explicit consent.[26] According to Antoinette Rouvroy, a member of the European Data Protection Supervisor's Ethics Advisory Group, Article 22 embodies an aspiration that is "both unrealistic and deeply paradoxical."[27] On the other hand, the Article 29 Working Party explains that Article 22 applies in relatively narrow circumstances. Moreover, member states of the EU have authority pursuant to Article 22(2)(b) to derogate the right, so long as appropriate protections are put in place.[28]

[21] For examples and an overview, see generally Mayer-Schönberger & Padova, *supra* note 3.

[22] Big Data, *supra* note 17, at 40-41.; *see also* Ann Cavoukian, David Stewart & Beth Dewitt, *Using* Privacy by Design *to Achieve Big Data Innovation Without Compromising Privacy*, Info. and Priv. Commc'n of Ontario 16 (June 10, 2014).

[23] GDPR, art. 22.

[24] GDPR, art. 22(1).

[25] Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, Article 29 Data Protection Working Party 21 (Oct. 3, 2017).

[26] Zarsky, *supra* note 2, at 1017.

[27] Antoinette Rouvroy, *Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data*, Council of Eur., Directorate Gen. of Hum. Rts. and Rule of L. 11 (Jan. 11, 2016).

[28] GDPR, art. 22(2)(c) ("[The right not to be subject to an automated decision shall not apply if the decision] is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.").

As this Part explored, several provisions of the GDPR have the potential to burden data-driven analytics. The burden will turn, in large part, on the interpretations ultimately adopted by regulators and the courts. While waiting for clearer guidance, however, companies must continue to operate. Below, we examine one method for companies to continue data-driven analytics despite substantive uncertainty in the GDPR: striving in good faith to comply by implementing an effective compliance program.

III. Mitigating Effects of Effective Compliance Programs

Despite authorizing astronomic penalties, the GDPR acknowledges that not all unlawful processing should be prosecuted to the fullest extent. In fact, the GDPR instructs regulators to consider several factors in deciding an appropriate fine.[29] These factors suggest that good-faith efforts to comply with the Regulation have an inoculating effect against severe penalties. One mechanism to demonstrate good-faith compliance is to design and enforce an effective compliance program.

Good-faith efforts to comply bear on intentionality and negligence and demonstrate serious contemplation of big data analytics' risks. Common sense suggests intentionally unlawful activity should be punished more harshly than unintentionally unlawful activity. Article 83(2)(b) incorporates that common sense into the GPDR.[30] According to the Article 29 Working Party, regulators shall look for "objective elements of conduct" when deciding whether intentional misconduct or negligence occurred.[31] hese objective elements might include "unlawful processing authori[z]ed explicitly by the top management hierarchy . . . in disregard for existing policies[,] . . . failure to read and abide by existing policies, human error, failure to check for personal data in information pub-

[29] GDPR, art. 83(2).

[30] GDPR, art. 83(2)(b) ("When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine . . . due regard shall be given to . . . the intentional or negligent character of the infringement."); *see also* Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679, Art. 29 Data Protection Working Party 12 (Oct. 3, 2017) ("It is generally admitted that intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine.") [hereinafter "Penalty Guidance"].

[31] Penalty Guidance, *supra* note 30, at 12.

lished, failure to apply technical updates in a timely manner, [and] failure to adopt policies."[32] Moreover, companies who demonstrably take their obligations under the GPDR seriously will likely receive leniency. Failures that "demonstrat[e] contempt for the provisions of the law" are more likely to be fined.[33] Regulators must also give "due regard [to] . . . the degree of responsibility of the controller" while accounting for obligations imposed under Article 25.[34] All these provisions were aptly summarized by the Article 29 Working Party: has a company "d[one] what it could be expected to do given the nature, the purposes or the size of the processing"?[35] Designing and enforcing an effective compliance program signals genuine respect for the purposes of the law, promotes compliance, responds to changes in the law, and assures regulators that companies have done what they can.

As covered above, the GDPR implicitly and explicitly endorses compliance programs as a way to limit or avoid penalties for unlawful activity entirely. Yet *pro forma* compliance programs belie the contempt of an organization for the protections of the GDPR. Thus, to demonstrate good-faith efforts, companies and regulators should seek effective compliance. An established body of law, found in the U.S. Federal Sentencing Guidelines for Corporations ("Sentencing Guidelines"), can be looked to in defining an effective compliance program.[36] American authorities use the Sentencing Guidelines to offer reduced fines, and even amnesty, for companies who, notwithstanding an effective compliance program, have violated the law.[37] Unlike the GDPR, however, the Sentencing Guidelines also offer seven elements that comprise an effective compliance program. To ensure they benefit from the GDPR's limited liability mechanism, controllers dealing with substantive uncertainty should look to the

[32] Penalty Guidance, *supra* note 30, at 12.

[33] Penalty Guidance, *supra* note 30, at 12.

[34] GDPR, art. 83(2)(d).

[35] Penalty Guidance, *supra* note 30, at 13.

[36] *See* Chapter 8 — Sentencing of Organizations, Guidelines manual, U.S. SENTENCING COMMISSION (2016), https://www.ussc.gov/guidelines/2016-guidelines-manual/2016-chapter-8 [hereinafter Sentencing Guidelines]. Because companies can be convicted under U.S. law, the Sentencing Guidelines summarize mitigating factors in determining appropriate fines after conviction.

[37] *See generally id.*; *see also* Memorandum from Paul J. McNulty, Deputy Attorney General, U.S. DEP'T OF JUSTICE, at 4. ("In . . . determining whether to bring charges, . . . prosecutors must consider . . . the existence and adequacy of the corporation's *pre-existing* compliance program." (emphasis in original)) [hereinafter McNulty Memorandum].

Sentencing Guideline as a framework for developing an effective compliance system.[38] The next Part explores what such a compliance system might entail.

IV. Seven Elements Of An Effective Compliance Program

Compliance programs are designed to prevent and detect undesirable conduct. Within the context of the GDPR, that entails following the law, as well as preventing and detecting objective elements of misconduct.[39] According to the Sentencing Guidelines, a compliance program means more than having processes in place; it requires promoting an organizational culture of lawful and ethical compliance.[40] In other words, *pro forma* compliance is insufficient. Under both the GDPR and the Sentencing Guidelines, *pro forma* compliance is unlikely to inspire a regulator to mitigate penalties. Beyond cultural change, the Sentencing Guidelines enumerate seven elements necessary to receive leniency. The following discussion explores each and, where appropriate, pontificates on what that may entail for a controller.

The first element of an effective compliance program requires establishing standards and procedures to prevent *and detect* unlawful ac-

[38] It is worth noting that other frameworks for effective compliance systems exist, such as ISO 19600:2014, https://www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en.

[39] As explained in Part III, *supra* , the Article 29 Working Party identified the following objective elements of misconduct: "unlawful processing authori[z]ed explicitly by the top management hierarchy . . . in disregard for existing policies[,] . . . failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, [and] failure to adopt policies." Penalty Guidance, *supra* note 30, at 12.

[40] Sentencing Guidelines, *supra* note 36, § 8B2.1(a) ("To have an effective compliance and ethics program, . . . an organization shall . . . promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law."); *see also* McNulty Memorandum, *supra* note 37, at 14 ("[T]he critical factors in evaluating any program are . . . whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives."); Speech of Elizabeth Denham, Commissioner of the U.K. Information Commissioner Office, given at the Data Protection Practitioner's Conference 2017 (Mar. 6, 2017), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/03/data-protection-practitioners-conference-2017/ ("It's about a framework that should be used to *build a culture of privacy that pervades an entire organisation*. It goes back to that idea of doing more than being a technician, and seeing the broader responsibility and impact of your work in your organisation on society." (emphasis added)).

tivity.[41] The GDPR, in turn, requires controllers to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."[42] Efforts to detect undesirable activity are necessary to assess the performance of preventative policies. While not explicitly found in the text of the GDPR, controllers should ensure they seek out unlawful conduct. Complicity and willful negligence should not be permitted.

For example, the GDPR demands Data Protection Impact Assessments ("DPIA") be conducted when processing is likely to result in a high risk to the rights and freedoms of natural persons.[43] For this provision, preventative controls may be implementing a procedure whereby mini-impact assessments are conducted for each new technology with the sole purpose of determining whether it requires a full DPIA. Detective controls, in turn, would entail a procedure to review, ex-post, completed mini-impact assessments to ensure they are being conducted appropriately.

The second element is concerned with vertical flow of information regarding the compliance program. Effective programs ensure information about and details of the compliance program flow between its day-to-day managers and governing authorities, such as boards.[44] Under the GDPR, data protection officers ("DPOs") have a similar obligation, though it does not explicitly require informing governing authorities.[45] To ensure governing authorities have sufficient understanding of their compliance program, they should be updated by DPOs, can be briefed by outside counsel, or can partake in director education programs.[46]

[41] Sentencing Guidelines, *supra* note 36, § 8B2(b)(1).

[42] GDPR, art. 24.

[43] GDPR, art. 35.

[44] Sentencing Guidelines, *supra* note 36, § 8B2.1(b)(2)(A)-(C).

[45] GDPR, art. 39(1)(a).

[46] Guidelines from the National Association of Corporate Director might prove useful in developing basic understanding of the relevant information and Director responsibility. *See, e.g.*, NACD Global Cyber Forum, NAT'L ASS'N OF CORP. DIRECTORS, https://www.nacdonline.org/Education/EventDetail.cfm?ItemNumber=45576 (last visited Nov. 29, 2017); *see also* Corey E. Thomas, The Corporate Director's Guide to GDPR, NAT'L ASS'N OF CORP. DIRECTORS (Aug. 15, 2017), https://blog.nacdonline.org/2017/08/directors-guide-to-gdpr/.

The third element requires companies use reasonable effort to avoid giving authority over the program to individuals who have a history of unlawful conduct or "other conduct inconsistent with an effective compliance . . . program."[47] The reasoning is clear: foxes should not guard hen houses. To satisfy this requirement, controllers should exercise reasonable diligence in selecting their DPO and data protection employees. Controllers should avoid hiring individuals who have been found previously to have intentionally violated the Regulation.

The fourth element requires periodic and practical communication of the organization's standards and procedures through "effective training programs" and "otherwise disseminating information" appropriate to the specific role.[48] The GDPR, in turn, tasks DPOs with "awareness-rising and training of staff involved in processing" with the goal of monitoring compliance.[49]

The fifth element requires taking reasonable steps to ensure the program is followed, its efficacy is regularly evaluated, and it includes a channel for resolving uncertainties and reporting violations anonymously.[50] Standard compliance techniques are helpful here, such as hiring outside counsel or consultants to review and certify the program, auditing databases and paper records, and implementing anonymous hotlines. Moreover, and particularly relevant to handling existing uncertainties, companies should implement procedures for incorporating new developments in European data protection laws into the organization's internal policies. Whether it be tracking new enforcement proceedings and judicial resolutions to new legislation, companies must ensure they stay on the "lawful" side of the spectrum. To do so, they must respond to the shifting ground quickly and effectively. Lethargic responses to authoritative interpretations of law throws any "good faith" finding into jeopardy, increasing the risk of penalty. The sixth element requires the program be promoted and enforced through rewards and punishments.[51] Basically, employees must be rewarded for good compliance and punished for unlawful activity. When employees are in a position to prevent unlawful activity, they must be punished for failing to take reasonable steps to pre-

[47] Sentencing Guidelines, *supra* note 36, § 8B2.1(b)(3).

[48] Sentencing Guidelines, *supra* note 36, § 8B2.1(b)(4)(A).

[49] GDPR, art. 39(1)(b).

[50] Sentencing Guidelines, *supra* note 36, § 8B2.1(b)(5)(A)–(C).

[51] Sentencing Guidelines, *supra* note 36, § 8B2.1(b)(6).

vent or detect it. Companies who overlook policy violations will have allowed, in the terms of the GDPR, "objective elements of misconduct" and be vulnerable to penalization in the event of unlawful processing.[52]

The seventh and final element demands a compliance program act like an algorithm; that is, change in response to feedback. Specifically, it must adapt to detected unlawful activities with the goal of preventing similar conduct in the future.[53] As part of their policies and standards, controllers should have a committee responsible for investigating potential unlawful activity and recommending changes to the compliance program as necessary.

V. Conclusion

To protect individual privacy and autonomy in a data-driven world, the European Union passed the GDPR, a gargantuan piece of legislation with many ambiguous definitions and exceptions. As written, the GDPR can be interpreted as outlawing recent technological developments such as Big Data and artificial intelligence. While such interpretations have yet to be authoritatively adopted, companies still must comply with the law or face exorbitant fees. In doing so, these actors operate vulnerable to over-zealous prosecution. Thankfully, despite existing uncertainty, companies can adopt effective compliance programs to mitigate any penalties levied. Drawing on the Sentencing Guidelines, this Note evaluated the necessary elements of an effective compliance program. For companies, this Note offers an existing body of law to reference when designing their compliance program. For regulators, this Note offers a legal basis for holding controllers to a higher standard than *pro forma* compliance—effective compliance.

[52] Penalty Guidance, *supra* note 30, at 12.

[53] Sentencing Guidelines, *supra* note 36, § 8B2.1(7).