General Data Protection Regulation (GDPR): Prioritizing Resources

Jennifer Dumas

INTRODUCTION

Imagine you are asked to mortgage your house and wager your life savings in a game of chance without knowing the rules. Now imagine your most risk-averse friend being asked to do the same thing. This is pretty much what lawyers have been charged with doing for the past few years in preparation for the GDPR.

Some companies appear to have been dismissive of the issue: "[GDPR] won't look much different from right now! That's why I am perplexed by the freakouts and meltdowns many are having over the European Union's (EU) General Data Protection Regulation (GDPR) May 25, deadline."[1] Other companies have developed entire business offerings around GDPR compliance.[2]

This Article will discuss and analyze the years of preparation for the GDPR and provide recommendations for dealing with the GDPR forevermore. It will assess whether the preparation and panic were worth it. In other words, was the time, expense, and distraction my peers and I expended and experienced over the past years proportionate to the requirements and impact of the GDPR? Further, was the high level of preparation and panic many legal departments in countless companies undertook and experienced appropriate now that we have had a chance to see the initial impact of the GDPR?

I. GENERAL GDPR OVERVIEW

Any analysis and assessment must begin with an overview of the GDPR. Although at the time of publication, the GDPR has been effective

1. Jen Brown, *What Will the Data Protection World Look Like Post GDPR Deadline?*, SUMO LOGIC (May 25, 2018), https://www.sumologic.com/blog/compliance/gdpr-data-protection-deadline/ [https://perma.cc/H7J7-HQWB].

2. *See, e.g.*, *Data Optimization and Privacy Specialists*, CALLIGO, https://calligo.cloud/ [https://perma.cc/5JZD-PVCX].

for over nine months, many companies are just now realizing the scope and breadth of the GDPR and that it applies to them. Interestingly, many continuing legal education (CLE) courses were still covering GDPR basics even months after its implementation.[3]

The GDPR is a piece of legislation that was approved by the European Union Parliament in April 2016 with a two-year buffer period before its provisions became effective on May 25, 2018.[4] It aims to give consumers control of their personal data collected by companies. Not only does it affect organizations located within the EU, but it also applies to companies outside of the region if they offer goods or services to, or monitor the behavior of, people in the EU.[5]

The GDPR regulates two types of data handlers: "controller[s]" and "processor[s]."[6] It protects identified or identifiable natural persons, each a "data subject."[7]

The GDPR recognizes the concept that data privacy is a fundamental right: "The protection of natural persons in relation to the processing of personal data is a fundamental right."[8] The GDPR provides a framework for protection of this right through seven key principles:

1. Lawfulness, fairness, and transparency[9]: Any information and communication relating to the processing of personal data must be easily accessible, easy to understand, and be presented using clear and plain language.[10]
    a. "Lawful" processing falls into five different categories:
        i. consent;
        ii. contract;

3. *See, e.g.*, *Global Privacy Summit 2019*, INT'L ASS'N PRIVACY PROF., https://iapp.org/conference/global-privacy-summit/ [https://perma.cc/ZK32-L7H4]; *49th Global Legal ConfEx & GDPR ConfEx, New York, USA, June 2019*, EVENTBRITE, https://www.eventbrite.com/e/50th-global-legal-confex-gdpr-confex-new-yorkusa-june-2019-tickets-49078820072 [https://perma.cc/XTN4-EC2F].

4. *GDPR FAQs: Frequently Asked Questions About GDPR*, EU GDPR.ORG, https://eugdpr.org/the-regulation/gdpr-faqs/ [https://perma.cc/3WBX-EEE4].

5. *Id.*

6. Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 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), art. 4, 2016 O.J. (L 119) 33 (EU) [hereinafter GDPR]. A Controller "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 . . . ." *Id.* art. 4(7), at 33. A Processor "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." *Id.* art. 4(8), at 33.

7. *Id.* art. 4(1), at 33.

8. *Id.* Recital 1, at 1.

9. *Id.* art. 5(1)(a), at 35.

10. *Id.*; *id.* Recital 39, at 7.

iii. legal obligations;
iv. public policy or public interest; and
v. legitimate interests that do not override the interests or fundamental rights of the data subject.[11]

b. If a company relies on consent, it must obtain an express and unambiguous "opt-in" consent from data subjects specific to each particular type of data it collects, unless an exception exists.[12] Specifically, consent:
   i. must be easy to withdraw;
   ii. can be revoked at any time;
   iii. must be opt-in and cannot be opt-out;
   iv. must be specific and not generalized;
   v. cannot be mandatory; and
   vi. may not extend to using personal data for a purpose beyond the reason it was collected. If personal data is used for a purpose beyond the reason it was collected, personal data should be pseudonymized or anonymized prior to use.

c. Finally, companies must have operational procedures in place to implement the specific consents or requests for withdrawal by data subjects.

2. Purpose limitation[13]: Data may only be used for the specific purpose identified by a company.

3. Data minimization[14]: Data collected must be relevant and limited to what is necessary in relation to the purposes for which it is processed. A company should not collect additional data that is not relevant to the processing need unless there is a legitimate purpose that was determined at the time of the data collection.

4. Accuracy[15]: Data must be accurate and kept current. Where data is inaccurate, it must be remedied and rectified without delay. Accuracy includes the following sub-elements:
   a. Right to be forgotten: Data subjects have a right to compel companies to erase their data and to stop third parties from processing the data.

---

11. *Id.* art. 6(1)(a)–(f), at 36.

12. *Id.* art. 6(1)(a), at 36. "In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards." *Id.* Recital 157, at 29.

13. *Id.* art. 5(1)(b), at 35.

14. *Id.* art. 5(1)(c), at 35.

15. *Id.* art. 5(1)(d), at 35.

   b. Right to data access: Data subjects have the right to request and receive detailed information on what data a company possesses about them, where that data is stored, and how it is utilized.
   c. Right to rectification: Data subjects have the right to change any incorrect information about themselves that is stored and accessed by a controller.
5. Storage limitation[16]: The storage of personal data should also be limited to the purposes for which the personal data was processed. Companies should take measures to ensure the storage of personal data held in backups is aligned to the stated purpose.
6. Integrity and confidentiality (security)[17]: Both controllers and processors must take clear steps to prevent unauthorized access to personal data, as well as the equipment used for the processing.[18]
   a. For security, controllers must take the following actions:
      i. provide clear notice of data collection, outline processing purposes and use cases, and define their data retention and deletion policies; and
      ii. establish and maintain a process to identify a breach in a timely manner, understand why it occurred, who was affected, and how to notify affected data subjects.
   b. Breach notifications: Both controllers and processors must notify a data subject within seventy-two hours of a data breach when the breach might compromise their privacy.
7. Accountability[19]: The controller is responsible for demonstrating compliance with the above requirements. Some examples include:
   a. creation and ability to demonstrate new policies, processes, and training;
   b. evidence of valid consents given by data subjects;
   c. detailed data record keeping; and
   d. possible appointment of a Data Protection Officer (DPO).

The above principles echo those of its predecessor, the Data Protection Act of 1998.[20] However, the GDPR carries with it a one–two punch of additional features that raise the stakes:

- it has a long reach and applies to any company doing business with EU citizens,[21] and

16. *Id.* art. 5(1)(e), at 36.
17. *Id.* art. 5(1)(f), at 36.
18. *Id.* Recital 39, at 7.
19. *Id.* art. 5(2), at 35.
20. Data Protection Act 1998, c. 29 (UK).
21. GDPR, *supra* note 6, art. 3(2), at 32.

- it specifies fines of up to 4% annual worldwide turnover or €20 million (whichever is greater), in the event of a breach.[22]

Within hours of the GDPR taking effect on May 25, 2018, Google, Facebook, Instagram, and WhatsApp received privacy complaints that could carry fines of up to $9.3 billion in total.[23]

II. HOW TO PREPARE FOR AND MAINTAIN COMPLIANCE WITH THE GDPR

Given the specific requirements of the GDPR and the high-stakes for non-compliance, companies had two years to prepare. Preparation affected virtually every aspect of an organization from Human Resources (HR) to Information Technology (IT) to Engineering to Sales. Preparation felt like looking into a crystal ball and seeking answers to questions not yet asked. This made it incredibly challenging to budget and commit resources—particularly in smaller companies with more limited resources. By way of comparison, "Fortune 500 firms have spent over $8 billion in their compliance efforts in the run-up to May 25, 2018."[24]

The costs incurred by all companies was staggering. Accordingly, the combination of broad scope and high uncertainty of requirements led many companies to take a "risk-based" approach. A risk-based approach involved assessing risks and requirements specific to a particular business unit, product line, or other aspect of the business, and then formulating a readiness program based on specific needs or highest needs only. Below is a sample readiness plan:

1. Top Priorities:
   a. Add GDPR language to customer contracts, including tailoring processor clauses to the company's standard customer terms.
   b. Create Data Protection Agreements (DPAs) and execute with all downstream vendors and sub-processors.
   c. Create Data Flow Maps—both for internal processes and including vendors and sub-processors. Map global personal data flows (typically with mapping questionnaires).
   d. Create an incident response plan in collaboration with the IT department.
   e. Update Internet privacy notice and cookie policy.
2. Next Level Priorities:

---

22. *Id.* art. 83(5)–(6), at 83.

23. Sean Keane, *GDPR: Google and Facebook Face up to $9.3B in Fines on First Day of New Privacy Law*, CNET (May 25, 2018), https://www.cnet.com/news/gdpr-google-and-facebook-face-up-to-9-3-billion-in-fines-on-first-day-of-new-privacy-law [https://perma.cc/C7TT-34Q8].

24. Mike Meikle, *GDPR'S First 150 Days Impact on the U.S.*, THREATPOST (Nov. 1, 2018), https://www.threatpost.com/gdprs-first-150-days-impact-on-the-u-s/138739/ [https://perma.cc/26CP-HRX2].

   a. Create employee privacy notice.
   b. Create employee data protection policy.
   c. Conduct employee GDPR training (practice tip: create a video recording that can be reused for all new-hires).
   d. Define and demonstrate data protection by design and default.
   e. Create record keeping plan.
3. Next Level Priorities:
   a. Assess need for DPO.
   b. Create data retention and destruction policy.
   c. Consider certification, if available.[25]

It is crucial for a company to have an internal playbook, including a rationale or justification for the risk-based decisions it made in completing its GDPR compliance program. The internal rationale will become even more important in the future. Because the GDPR is new, it is still unclear how it will be enforced. "There is a general lack of agreement about what exactly GDPR compliance is . . . [i]n the U.S., chief corporate counsels are unsure if their newly rewritten privacy policies are GDPR-compliant."[26]

After building a GDPR program, a company must then maintain it. The Accountability Principle of the GDPR requires ongoing ability to demonstrate compliance.[27] Once counsel successfully launches a GDPR compliance program, hand the exhausted counsel some vitamins because their work has just begun. Maintenance may include both ongoing checks and continual improvements. Some suggestions for maintenance steps include the following:

1. Engage an auditor to audit and check existing processes and procedures.
2. Consider maintenance program offerings by third parties.
3. Track regulations.
4. Operationalize and streamline processes.
5. Categorize and stack-rank vendors according to perceived risk.

---

25. As of publication, there is no official GDPR certification:

> [The Information Commissioner's Office] has no plans to accredit certification bodies or carry out certification at this time, although the GDPR does allow this. Currently, there are no approved certification schemes or accredited certification bodies for issuing GDPR certificates. Once the certification bodies have been accredited to issue GDPR certificates, you will find this information on ICO's and UKAS's websites.

Certification, INFO. COMMISSIONER'S OFF. (Feb. 12, 2019), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/certification/ [https://perma.cc/GCD8-WHHZ].

26. Meikle, *supra* note 24.

27. GDPR, *supra* note 6, art. 5(2), at 36.

6. Maintain an internal business owner for the process with visibility by executive suite and board of directors.
7. Develop and demonstrate a process for purging inappropriate data in systems.

III. ONE KEY TO COMPLIANCE: KNOW YOUR BUSINESS

As important as understanding general GDPR requirements is understanding how those requirements apply to and/or impact your business. For example, the GDPR contains many specific statements and provisions encouraging and validating the broad use of personal data for research and scientific purposes, thus limiting its scope and application in certain circumstances. "[T]he processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research."[28] In addition to this aspirational statement, the decretal text of the GDPR includes several express statements pertaining to research-based and scientific use of personal data.

Accordingly, the GDPR aims to encourage innovation, as long as organizations implement appropriate safeguards and the use is necessary "for the performance of a task carried out for reasons of public interest."[29] In other words, the GDPR contemplates expanded use of personal data for certain public policy purposes including scientific research, as long as the user of such personal data has a legitimate or compelling need for the data and has taken appropriate steps to safeguard the data.

Article 89 of the GDPR clarifies that a party may process personal data if it is in the public interest or for scientific research, historical research, or statistical purposes. Article 89 is referenced in several other sections of the GDPR, as discussed further below, and appears to be the foundation for many expanded uses of personal data. Importantly, Article 89 makes clear that expanded use of personal data must be justified by a balancing test; restricting use or access to the personal data would "render impossible or seriously impair the achievement of the specific purposes"[30] and a controller or processer must maintain "appropriate safeguards."[31]

For example, if a controller uses a data subject's personal data for scientific or research purposes, it does not necessarily need to obtain consent or limit its use of such personal data to an identified purpose, but

28. *Id.* Recital 159, at 30.
29. *Id.* art. 21(6), at 46.
30. *Id.* art. 89(3), at 85.
31. *Id.* art. 89(1), at 84–85.

it *does* still need to be open and transparent to the greatest extent possible about how that data will be used.

> Although controllers are not required to obtain the data subject's consent for all processing for research purposes, they remain bound by the GDPR's notice requirements. Article 12(1) requires controllers to "take appropriate measures" to inform data subjects of the nature of the processing activities and the rights available to them. Controllers are required to provide this information in all circumstances, regardless of whether consent is the basis for processing, "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (Article 12(1)).[32]

In fact, some commentators have gone so far as to opine that the GDPR does not change existing processes and policies at scientific and research institutions.

> Organisations need to be lawful, fair and transparent when processing or controlling the processing of personal data. However, the new legislation does not impede research. It reflects current good practice in research, through the safeguards that apply to all research using personal data. If your organisation is already using good practice under current data protection legislation, you will need to make relatively few changes to your policies and practices.[33]

GDPR Chapter 3, Articles 12 through 23 expound on the seven key principles discussed above and address in detail the specific rights of a data subject. However, exceptions to those rights exist, which allow expanded use of personal data. Below is an assessment of which of those rights include exceptions for scientific or research purposes, references to GDPR Article 89 or both:

Article 12—Transparency: Controllers must provide clear notice of data collection, outline processing purposes and use cases, and define their data retention and deletion policies. No express exceptions, though note general ease of transparency requirements in connection with the safeguarding of public safety and in the public interest.[34]

Article 13—Obligation to provide information when information is collected from a data subject: Recital 62 clarifies that the obligation to

---

32. Gabe Maldoff, *How GDPR Changes the Rules for Research*, INT'L ASS'N PRIVACY PROF. (Apr. 19, 2016), https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/ [https://perma.cc/273V-YCYX].

33. *Data Protection and Information Governance*, HEALTH RES. AUTHORITY, https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/ [https://perma.cc/87DC-R496].

34. GDPR, *supra* note 6, Recital 73, at 14.

provide information is "not necessary . . . where the provision of information to the data subject provides to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes."[35]

Article 14—Obligation to provide information when information is collected from a third party: Article 14 also references Recital 61, but includes an express exception as well:

> Paragraphs 1 to 4 shall not apply where and insofar as . . . (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1).[36]

Article 15—Right of Access: Article 89(2) offers an explicit exception. "Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21."[37]

Article 16—Right to Correct: Article 89(2) offers an explicit exception. "Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21."[38]

Article 17—Right to Erasure: Article 17(3)(d) offers an explicit exception. "Paragraphs 1 and 2 shall not apply to the extent that processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)."[39]

Article 18—Right to Restriction of Processing: Article 89(2) offers an explicit exception. "Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21."[40]

---

35. *Id.* Recital 62, at 12.

36. *Id.* art. 14(5)(b), at 42; *id.* Recital 62, at 12.

37. *Id.* art. 89(2), at 85.

38. *Id.*

39. *Id.* art. 17(3)(d), at 44; *id.* Recital 65, at 12–13 (supporting the conclusion that the "retention of the personal data should be lawful where it is necessary . . . for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes").

40. *Id.* art. 89(2), at 85.

Article 21—Right to Object to Use of Data: Article 21(6) offers an explicit exemption. "Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest."[41]

Other examples of how the GDPR allows expanded use of personal data for research purposes include the following:

1. Exceptions to restrictions on secondary processing and processing sensitive categories of data.[42]
2. Exceptions to consent requirement.[43]
3. Exceptions to restrictions on transfer to third countries without any other transfer mechanism in place.[44]
4. Exceptions to purpose limitation.[45]
5. Exceptions to prohibition on processing sensitive data revealing racial or ethnic origin, religious or political beliefs, as well as genetic, biometric, and health data.[46]

Accordingly, the GDPR states clearly and repeatedly that it should not restrict access to personal data for certain public policy and science-based uses. Similar to the other GDPR principles, it remains unclear how these exceptions and policy statements will be interpreted by data subjects and courts alike. What is clear, however, is that the GDPR is intended to harmonize the use of personal data with other, equally important, fundamental rights and privileges: "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."[47]

---

41. *Id.* art. 21(6), at 46.

42. *Id.* art. 6(4), at 37; *id.* Recital 50, at 9–10. Sensitive data is any data that reveals (i) racial or ethnic origin; (ii) political opinions; (iii) religious or philosophical beliefs; (iv) trade union membership; (v) genetic data; (vi) biometric data; (vii) data concerning health or a person's sex life and/or sexual orientation. *GDPR Sensitive and Non-Sensitive Data: A Distinction with a Difference*, CRITEO (Dec. 21, 2017), https://www.criteo.com/insights/gdpr-sensitive-non-sensitive-data-distinction-difference/ [https://perma.cc/R9C9-FCEA]; *see also* GDPR, *supra* note 6, art. 9(1), at 38.

43. GDPR, *supra* note 6, art. 6(1)(f), at 36; *id.* Recital 47, at 9; *id.* Recital 157, at 29.

44. *Id.* art. 49(1), at 64; *id.* Recital 113, at 21.

45. *Id.* art. 5(1)(b), at 35.

46. *Id.* art. 9(2)(j), at 39; *see also id.* art. 89, at 84–85.

47. *Id.* Recital 4, at 2.

These exceptions are crucial to understand for anyone counseling a research institution. Similar exceptions may exist within the GDPR for other industries or uses of personal data. In order to develop a risk-based GDPR compliance program, it therefore is important for an attorney to understand how the GDPR applies, both generally and specifically, to their applicable use case.

IV. LOOKING FORWARD: PROJECTED IMPACT OF THE GDPR

While there is growing clarity about building a GDPR program, both consumers and users, as well as controllers and processers, remain uncertain about the how the GDPR will be applied. Two likely areas where the GDPR will continue to evolve are consumer and individual activism and regulatory incompatibility.

A. Consumer Activism

With greater rights to information and accountability, many individual users have started complaining about the use of their data or requesting that their data be deleted by a company. These user requests are often based on incomplete knowledge of the GDPR and can lead to over-reaching by users, which could actually slow enforcement and understanding of the GDPR. For example, in July 2018 the European Consumer Organisation (BEUC) released an article explaining how its research team had used artificial intelligence to scan and analyze privacy policies of fourteen leading online companies for GDPR compliance.[48] BEUC concluded that "none of the analysed policies fully met the requirements of the GDPR."[49] Not only did this consumer group conduct its own legal research, it also indicated that it would consider seeking enforcement based on its legal conclusions. "BEUC will bring this research to the attention of the data protection authorities and will continue monitoring market developments closely. We do not rule out taking further legal actions as appropriate."[50] Ironically, this consumer activism could slow enforcement by overwhelming local authorities. "[The GDPR] has raised security awareness, but right now Data Protection Authorities are overwhelmed with complaints, and there is significant confusion around the law."[51]

---

48. *Research Suggests Privacy Policies of Leading Online Companies Do Not Fully Respect GDPR*, BEUC (Apr. 7, 2018), https://www.beuc.eu/publications/research-suggests-privacy-policies-leading-online-companies-do-not-fully-respect-gdpr/html [https://perma.cc/99MZ-5S5W].

49. *Id.*

50. BEUC, USING ARTIFICIAL INTELLIGENCE TO EVALUATE PRIVACY POLICIES "CLAUDETTE MEETS GDPR" PROJECT Q&A 3 (2018), https://www.beuc.eu/publications/beuc-x-2018-065_faq_-_artificial_intelligence_meets_gdpr.pdf [https://perma.cc/H7JM-AFN2].

51. Meikle, *supra* note 24.

B. Regulatory Incompatibility

The next phase of GDPR analysis and assessment may also raise awareness about certain regulatory incompatibilities that may work counter to the intent of GDPR. One example of this is Artificial Intelligence (AI) Technology.[52] With AI Technology, the more data, the better. As important as quantity, however, is quality. Machines need personal data if such data is material to or relevant to an analysis or outcome. "Machine learning is looking for patterns in data. If you start with racist data, you will end up with even more racist models."[53] Without the ability to assess personal information, AI Technology will be limited and perhaps even enable bias or racial profiling. AI Technology still needs humans to feed data and provide interpretations. Countries that have looser privacy considerations have a huge advantage in the development of AI Technology. Tsuhan Chen, chief scientist for AI Singapore, a national program to foster AI research, and a deputy president at the National University of Singapore, was interviewed on this subject by the *Wall Street Journal*. Dr. Chen said, "China is dominating in machine learning. They are leveraging the availability of data. There are definitely more people to crunch data, and there are more people providing data."[54] The GDPR is designed to restrict access to data, but data, even racist or discriminatory data, is necessary to train an AI model to recognize and account for racism or discrimination.

For example, AI-based facial recognition systems in the United States tend to identify the faces of women and people with dark skin less

---

52. AI Technology can include, for example:

- Neural networks and deep learning (e.g., brain modeling, time series prediction, and classification),
- Evolution and genetic computation (e.g., genetic algorithms and genetic programming),
- Reinforcement learning,
- Computer vision (e.g., object recognition and image understanding),
- Expert systems (e.g., decision support systems and teaching systems),
- Speech and audio processing (e.g., speech recognition and production),
- Natural language processing (e.g., machine translation),
- Planning (e.g., scheduling and game playing),
- Audio and video manipulation technologies (e.g., voice cloning and deepfakes),
- AI cloud technologies, or
- AI chipsets.

53. David Rotman, *AI Savants, Recognizing Bias, and Building Machines That Think like People*, MIT TECH. REV. (Mar. 26, 2018) (quoting Oren Etzioni), https://www.technologyreview.com/s/610621/emtech-digital-oren-etzioni-brenden-lake-timnit-gebru/ [https://perma.cc/AP5C-7FVW].

54. Phred Dvorak, *Which Country Is Winning the AI Race—the U.S. or China?*, WALL ST. J. (Nov. 12, 2018), https://www.wsj.com/articles/which-country-is-winning-the-ai-racethe-u-s-or-china-1542039357.

accurately than people with lighter skin.[55] Companies such as Amazon have cited privacy concerns to justify their refusal to share information about whether their AI Technology contains bias.

> Amazon has come under intense scrutiny by federal lawmakers, the American Civil Liberties Union, shareholders, employees and academic researchers for marketing [Amazon's facial-recognition technology] Rekognition to law-enforcement agencies. . . . Amazon, citing customer confidentiality, has also declined to answer questions from federal lawmakers about which government agencies are using Rekognition or how they are using it.[56]

As the GDPR evolves, data subjects and data users alike should remain vigilant and sensitive to unintended consequences or applications of the GDPR that could actually contradict its intended purpose.

CONCLUSION

The GDPR is an ambitious achievement and represents years of work and input by innumerable contributors. It will be the privacy lodestar for the foreseeable future. It has affected virtually every company in the United States and Europe, and there are as many interpretations of its impact as there are lawyers. In some ways, the attention the GDPR has received has thwarted its impact. "[C]ompanies have weighed the cost of compliance with the potential for realizing a fine, and have so far taken a wait-and-see approach."[57]

Nevertheless, the GDPR is here to stay and will become the new normal. Already, other jurisdictions are modeling their privacy laws after the GDPR's principles: "California was influenced by GDPR when Governor Jerry Brown proposed and passed the California Consumer Privacy Act (CCPA). . . . The CCPA is scheduled to go into effect on January 1, 2020."[58]

The GDPR could also provide guidance in areas such as assessing export control regulations of Artificial Intelligence Technology.[59] The next several months will be like the "Wild West" with various parties jockeying for leadership positions and racing to the courthouse. For these

---

55. *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACHINE LEARNING RES. 1 (2018).

56. Natasha Singer, *Amazon is Pushing Facial-Recognition Technology That a New Study Says Could Be Biased*, SEATTLE TIMES (Jan. 24, 2019), https://www.seattletimes.com/business/amazon/amazon-is-pushing-facial-technology-that-a-study-says-could-be-biased/.

57. Meikle, *supra* note 24.

58. *Id.*

59. Allen Institute for Artificial Intelligence, Comment Letter on Proposed Rule on the Review of Controls for Certain Emerging Technologies (Feb. 14, 2019), https://www.regulations.gov/document?D=BIS-2018-0024-0074.

reasons, in-house counsel would be well-advised to continue focusing on GDPR preparation and compliance and devoting resources to continual attention and maintenance.