MEDICAL DEVICE INNOVATION IN THE WAKE OF GDPR AND THE BIG FIVE DATA AND PRIVACY LEGISLATION

*Kaitlyn Coutcher**

INTRODUCTION

Technological change underpins many developments in agriculture, communication, transportation, computing, research, and more. The opportunities for technology to advance healthcare are abundant, not just for improving patient outcomes, but also for healthcare providers and the entire healthcare ecosystem. For example, incorporation of cutting-edge technologies and advanced software into medical devices, as has been done in artificial intelligence and machine learning-enabled medical devices, can facilitate earlier disease detection, improve and personalize diagnostics and therapeutics, and bring unprecedented efficiency and precision into the operating room.[1] However, pain, suffering, and death from disease still plague patients worldwide. Likewise, many tools in the operating room are suboptimal, with much room for improvement.[2] Cumbersome regulatory requirements on the medical device industry have slowed development, prolonging the time between innovation and widespread adoption of new medical technologies. Despite the existence of innovative medical devices, "their delayed adoption means that patients may miss out on potential benefits, leading to suboptimal outcomes and increased healthcare costs."[3]

Beyond ever-evolving medical device regulations, governments around the world are introducing new data and privacy legislation to "regulate data usage to

* J.D. Candidate, University of Toledo College of Law, anticipated May 2026. I would like to express sincere gratitude to my faculty advisor, Professor Deborah Machalow, and my Note and Comment Editor, Rachel Anderson, for their insightful guidance and critical feedback throughout the writing process for this Comment. I would also like to thank my family for never ceasing to believe in me. This piece is written in the author's personal capacity and should not be interpreted to reflect the views of the author's employer.

1. David B. Olawade et al., *Artificial Intelligence in Healthcare Delivery: Prospects and Pitfalls*, 3 J. MED., SURGERY, & PUB. HEALTH 1, 1 (2024).

2. INST. OF MED. OF THE NAT'L ARCHIVES, PUBLIC HEALTH EFFECTIVENESS OF THE FDA 510(K) CLEARANCE PROCESS: BALANCING PATIENT SAFETY AND INNOVATION: WORKSHOP REPORT 17 (Theresa Wizemann ed., 2010).

3. Andrew Landsman, *Closing the Gap: Medical Device Innovation, Frontline Healthcare Workers, and the Role of AI*, HUSCH BLACKWELL (Mar. 5, 2024), https://www.healthcarelawinsights.com/2024/03/closing-the-gap-medical-device-innovation-frontline-healthcare-workers-and-the-role-of-ai/.

prevent exploitation of consumer data."[4] Europe has implemented the "Big Five" pieces of data legislation (the Data Governance Act, Digital Services Act, Digital Markets Act, Data Act, and Artificial Intelligence Act), in addition to the infamous General Data Protection Regulation (GDPR), which is the most stringent data privacy and security law in the world.[5] Medical device companies are not only burdened by costly and resource-heavy regulatory requirements for each country where they seek to distribute their devices, but now must also contend with new, heightened standards for safeguarding privacy and data protection where the law is ambiguous and regulators fail to provide adequate guidance.

This Comment will begin with a brief history of innovation in the medical device industry along with an introduction to the complex regulatory hurdles that companies face when bringing new technologies to market. Next, this Comment will analyze the trends, impacts, and effects of GDPR and the "Big Five" data and privacy legislation on the medical device industry's ability to implement cutting-edge advancements in surgical medical devices. Finally, this Comment will conclude with a call for policymakers to temper the economic impacts of data and privacy regime compliance to account for the adverse effects on innovation and the accessibility of valuable medical technologies.

I. HISTORY OF MEDICAL DEVICE INNOVATION

The medical device industry produces a vast array of products, ranging from conventional surgical tools like blades and scalpels, to implantable devices like artificial joints, to advanced surgical robotic systems.[6] The industry and its breadth of products play a crucial role in the development of new medical technology innovations that aim to further improve illness diagnosis and treatment.[7] Defined broadly, a medical device "can be any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination for a medical purpose."[8] Medical devices are means to specific ends: prevention of disease, correction of disease, or rehabilitation from disease.[9]

Creative innovation in the industry can arise through identifying a need in the market for a new medical device based on inputs from practicing physicians with

4. Aska Fujimori-Smith, Note, *Analysis of Global Data Privacy Regulations and How Transnational Companies Are Impacted*, 40 SANTA CLARA HIGH TECH. L. J. 91, 96 (2024).

5. Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?*, GDPR EU, https://gdpr.eu/what-is-gdpr/ (last visited Mar. 10, 2026).

6. FRANCIS J. CROSSON, MEDPAC REPORT TO THE CONGRESS: MEDICARE AND THE HEALTH CARE DELIVERY SYSTEM 207 (2017).

7. *Id.*

8. *Medical Devices*, WORLD HEALTH ORG., https://www.who.int/health-topics/medical-devices#tab=tab_1 (last visited Mar. 10, 2026).

9. Medical devices aid in the prevention, correction, and rehabilitation of diseases by enabling early detection through screening and diagnostic tools, providing therapeutic interventions to treat existing conditions, and supporting the restoration of function in affected body parts allowing people to return from a dependent status to a functional status. Samuel O. Thier, *New Medical Devices and Health Care*, *in* NEW MEDICAL DEVICES: INVENTION, DEVELOPMENT, AND USE 3 (Karen B. Ekelman ed., 1988).

firsthand experience about what works and what does not.[10] Insights into the basic mechanism of disease from physicians may be translated into new therapeutic modalities, providing companies with an opportunity to replace outdated tools with new technology and ensuring that patients will benefit to the maximum extent possible from innovation, including inventions of new devices and modifications of existing ones.[11]

In general, small, entrepreneurial companies are engaged in research and development of new medical devices for specific therapeutic uses.[12] These smaller companies serve as "innovation catalysts" and foster an environment of entrepreneurial drive, where the innovator is the key decision-maker and can take risks based upon their first-hand knowledge of the technology and its possible applications.[13] Larger corporations tend to acquire smaller innovative companies and their products, thereby providing the larger company with the innovation it needs to grow its market share while providing the small company with needed capital and access to expertise in scaling up production.[14] However, the decision-makers in larger corporations are often several management layers removed from the innovators and lack the reassurance gained from direct involvement in the innovative process.[15] This results in the decision-makers in larger corporations lacking the tools to properly assess risks and leads to their tendency to avoid the risks altogether.[16]

Upon introduction of a device to the market, a company enters into the iterative innovation lifecycle involving implementation of incremental changes to its products and processes based on the consumer experience and results from device use. After acquiring a small innovator, larger companies are faced with the ongoing duty to maintain compliance with standards and regulations and to continue the lifecycle of the device, which involves modifying, upgrading, and improving devices that were originally created by the innovation catalyst to offer the best product performance and features. However, to roll out new technologies in marketed devices and to disrupt the status quo, companies face a towering hurdle: regulatory requirements.[17] If the regulatory process is too difficult, time-consuming, or costly, it will deter even the most talented and creative innovators.[18]

---

10. INST. OF MED. OF THE NAT'L ARCHIVES, *supra* note 2, at 17.

11. Thier, *supra* note 9, at 5; Edward B. Roberts, *Technological Innovation and Medical Devices*, *in* NEW MEDICAL DEVICES: INNOVATION, DEVELOPMENT, AND USE 35, 36 (Karen B. Ekelman ed., 1988).

12. Alan Kahn, *The Dynamics of Medical Device Innovation: An Innovator's Perspective*, *in* THE CHANGING ECONOMICS OF MEDICAL TECHNOLOGY 89, 90 (Annetine C. Gelijns & Ethan A. Halm, eds., 1991).

13. *Id.*; INST. OF MED. OF THE NAT'L ARCHIVES, *supra* note 2, at 18.

14. INST. OF MED. OF THE NAT'L ARCHIVES, *supra* note 2, at 18-19.

15. Kahn, *supra* note 12, at 90.

16. *Id.*

17. *See CDRH International Affairs*, U.S. FOOD & DRUG ADMIN. (June 25, 2025), https://www.fda.gov/medical-devices/cdrh-international-affairs (generally explaining that international regulatory agencies ensure medical devices meet safety standards and regulations that vary from country to country).

18. INST. OF MED. OF THE NAT'L ARCHIVES, *supra* note 2, at 21.

Companies may avoid investing in projects that will face significant regulatory hurdles, preventing many valuable ideas and technologies from ever reaching patients.[19]

A. The Regulatory Hurdles Hindering Medical Device Innovation

Medical devices are highly regulated, with safety standards and regulations for medical devices varying from country to country.[20] These standards and regulations exist to ensure patient safety and device effectiveness to improve patient health.[21] Therefore, regulators play a significant role in patients' access to new technologies. These regulatory systems must be predictable and reasonable,[22] in no small part because innovation catalysts look for guidance from the regulatory system as they try to advance concepts from mere ideas to the product stage.

1. The United States

In the United States, all medical products are regulated by a single agency, the U.S. Food and Drug Administration (FDA).[23] The FDA acquired extensive premarket and post-market regulatory authority and oversight over medical devices through Congress's enactment of the Medical Device Amendments of 1976 (MDA).[24] The MDA extended the coverage of the Federal Food, Drug, and Cosmetic Act (FD&C Act), 21 U.S.C. §§ 301-399, to medical devices.[25] Enacted "to provide for the safety and effectiveness of medical devices intended for human use,"[26] the new regulatory regime under the MDA created a three-class, risk-based classification scheme based on the degree of health risk the device poses to the public.[27]

Considering the vast array of products in the medical device industry and the potential risks associated with them, the regulation of medical devices in the U.S.

---

19. Ariel Dora Stern, *Innovation Under Regulatory Uncertainty: Evidence from Medical Technology*, J. PUB. ECON., Jan. 2017, at 23.

20. *CDRH International Affairs*, *supra* note 17.

21. Bijaya Chettri & Ramya Ravi, *A Comparative Study of Medical Device Regulation Between Countries Based on Their Economies*, 21 EXPERT REV. MED. DEVICES 467, 468 (2024).

22. INST. OF MED. OF THE NAT'L ARCHIVES, *supra* note 2, at 21.

23. *Products and Medical Procedures*, U.S. FOOD & DRUG ADMIN. (Oct. 5, 2023), https://www.fda.gov/medical-devices/products-and-medical-procedures.

24. Susan Bartlett Foote, *The Impact of Public Policy on Medical Device Innovation: A Case of Polyintervention*, *in* THE CHANGING ECONOMICS OF MEDICAL TECHNOLOGY 69, 76 (Annetine C. Gelijns & Ethan A. Halm, eds., 1991).

25. Stengel v. Medtronic Inc., 704 F.3d 1224, 1226 (9th Cir. 2013) (en banc); Higginbottom v. Dexcom, Inc., 744 F. Supp. 3d 1058, 1079 (S.D. Cal. 2024); *see also* Riegel v. Medtronic, Inc., 552 U.S. 312, 315-16 (2008) (describing the rigorous regime instituted by Congress through the passage of the MDA, which established various levels of detailed federal oversight based on the risks that the medical device presents).

26. Medical Devise Amendments of 1976, Pub. L. No. 94-295, 90 Stat. 539 (codified as amended at 21 U.S.C. § 301).

27. Medtronic, Inc. v. Lohr, 518 U.S. 470, 476-77 (1996).

is complex.[28] Medical device manufacturers are subject to a range of regulatory controls to ensure that devices are free from defects, accurately labeled, and meet established standards for device safety and effectiveness for their intended use.[29] The extent of regulatory controls and oversight is based on the device's risk classification, which ranges from Class I to Class III.[30] Devices that present no unreasonable risk of illness or injury and are simpler in design are designated as Class I, meaning they are subject only to minimal regulation by "general controls" to provide reasonable assurance of safety and effectiveness.[31] Most low-risk Class I devices, including, for example, elastic bandages, examination gloves, and most hand-held surgical instruments, can be marketed without prior FDA review.[32] Devices that are potentially more harmful are designated as Class II; manufacturers of such devices must comply not only with general controls, but also with federal performance regulations known as "special controls"[33] to demonstrate only that they are "substantially equivalent" to an existing, legally marketed device through a Premarket Notification 510(k) submission before being marketed.[34] The FDA's review of devices for substantial equivalence is known as the § 510(k) process.[35] Examples of Class II devices include powered wheelchairs, infusion pumps, and surgical drapes.[36] Finally, devices that pose the most significant risk of illness or injury are placed in Class III, the most restrictive classification.[37] Before a new Class III device may be introduced to the market, the manufacturer must provide

28. AMANDA K. SARATA, CONG. RSCH. SERV., R47374, FDA REGULATION OF MEDICAL DEVICES 1 (2023).

29. *Id.*

30. *Overview of Device Regulation*, U.S. FOOD & DRUG ADMIN. (Jan. 31, 2024), https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/overview-device-regulation.

31. *Lohr*, 518 U.S. at 477 (quoting 21 U.S.C. § 360c(a)(1)(A) (1976)); As a note on terminology, "[g]eneral controls are the regulatory requirements that all medical devices are subject to and, taken together, are intended to ensure that all devices meet the standard of reasonable assurance of safety and effectiveness." SARATA, *supra* note 28, at 6; General controls "include provisions that relate to adulteration; misbranding; device registration and listing; premarket notification; banned devices; notification, including repair, replacement, or refund; records and reports; restricted devices; and good manufacturing practices." *General Controls for Medical Devices*, U.S. FOOD & DRUG ADMIN. (Dec. 15, 2023), https://www.fda.gov/medical-devices/regulatory-controls/general-controls-medical-devices.

32. *Class I and Class II Device Exemptions*, U.S. FOOD & DRUG ADMIN. (July 1, 2025), https://www.fda.gov/medical-devices/classify-your-medical-device/class-i-and-class-ii-device-exemptions; *Information Sheet Guidance for IRBs, Clinical Investigators, and Sponsors: Frequently Asked Questions About Medical Devices*, U.S. FOOD & DRUG ADMIN. 2 (Jan. 2006).

33. *Lohr*, 518 U.S. at 477 (quoting 21 U.S.C. § 360c(a)(1)(B) (1976)); *Regulatory Controls*, U.S. FOOD & DRUG ADMIN. (Mar. 27, 2018), https://www.fda.gov/medical-devices/overview-device-regulation/regulatory-controls#special ("Special controls are usually device-specific and include: Performance standards, Postmarket surveillance, Patient registries, Special labeling requirements, Premarket data requirements, [and] Guidelines.").

34. *Overview of Device Regulation*, *supra* note 30.

35. The term "510(k) submission" comes from Section 510(k) of the Federal Food, Drug, and Cosmetic Act (FD&C Act). Riegel v. Medtronic, Inc., 552 U.S. 312, 317 (2008).

36. *Information Sheet Guidance for IRBs, Clinical Investigators, and Sponsors, supra* note 32, at 2.

37. *Overview of Device Regulation*, *supra* note 30.

the FDA with a "reasonable assurance" through the rigorous premarket approval (PMA) process that the device is both safe and effective.[38] Examples of Class III devices include replacement heart valves, silicone gel-filled breast implants, and implanted cerebellar stimulators.[39]

In implementing the MDA, the FDA adopted regulations that delineate, to some extent, the data requirements for a 510(k) notification versus a PMA application.[40] For a PMA application, "[m]anufacturers must submit detailed information regarding the safety and efficacy of their devices, which the FDA then reviews, spending an average of 1,200 hours" per application.[41] If the FDA determines that the application contains "sufficient valid scientific evidence to provide reasonable assurance that the device is safe and effective for its intended use," the agency issues a PMA approval order.[42]

On the other hand, for a 510(k) notification, safety and effectiveness data are not explicitly required. Manufacturers must only provide information supporting their claim of substantial equivalence to an existing legally marketed predicate device, which is a comparative standard that does not require a *de novo* demonstration of safety and effectiveness.[43] To establish substantial equivalence, manufacturers show the new and predicate devices have the same intended use and any differences in technological characteristics do not raise different questions of safety and effectiveness.[44] If the FDA agrees that the new device is "substantially equivalent" to a legally marketed predicate device for which premarket approval is not required, "the agency provides 510(k) clearance for the device to be marketed" and classifies it like its predicate, subjecting it to the same regulatory controls, as well.[45]

The FDA's regulation of medical devices continues after they enter the market. One related requirement is the Quality System Regulation (QSR), which requires manufacturers to have an operational system to document and assess design changes.[46] Once a device receives initial FDA approval of a PMA application or clearance of a 510(k) notification, the manufacturer must evaluate any changes to its products or processes using a risk-based approach to determine

38. Hrymoc v. Ethicon, Inc., 297 A.3d 1245, 1256 (N.J. 2023) (quoting *Lohr*, 518 U.S. at 477); *see also* 21 U.S.C. § 360e(d)(2) (defining Class III medical devices and establishing the general requirements for premarket approval of such devices).

39. *Information Sheet Guidance for IRBs, Clinical Investigators, and Sponsors, supra* note 32, at 2.

40. Jonathan S. Kahan, *Premarket Approval Versus Premarket Notification: Different Routes to the Same Market*, 39 FOOD DRUG COSM. L.J. 510, 515 (1984).

41. *Lohr*, 518 U.S. at 477.

42. SARATA, *supra* note 28, at 20.

43. Kahan, *supra* note 40, at 517.

44. Substantial equivalence must be proven before a new medical device can be marketed in the United States through the FDA's 510(k) process. *Premarket Notification 510(k)*, U.S. FOOD & DRUG ADMIN. (Aug. 22, 2024), https://www.fda.gov/medical-devices/premarket-submissions-selecting-and-preparing-correct-submission/premarket-notification-510k.

45. SARATA, *supra* note 28, at 9.

46. Quality System Regulation, 21 C.F.R. § 820 (2026); *see* Etienne Nichols, *21 CFR Part 820: Ultimate Guide to FDA's Quality System Regulation (QSR) for Medical Devices*, GREENLIGHT GURU (Feb. 13, 2023), https://www.greenlight.guru/blog/21-cfr-part-820.

the extent to which the safety and effectiveness of the device is or could be impacted.[47] A risk-based assessment entails identification and assessment of all possible risks associated with a product or process change and then tailoring the submission determination based on the severity of those risks and their probability of occurrence.[48] Modifications to medical devices may warrant repeated verification or validation testing activities, as even seemingly minor invalidated alterations could adversely affect performance or safety in unpredictable ways.[49] The nature of the new data required to demonstrate the safety and effectiveness of the modified device generally indicates the type of new regulatory filing requiring the FDA's review and prior approval before implementation.[50] In general, greater technological changes embedded in a modified product raise the product's risk profile, demanding more effort for validation and increasing the need for regulatory oversight.

Beyond the data requirements for regulatory filings, Congress enacted the Medical Device User Fee and Modernization Act of 2002 (MDUFMA), which amended the FD&C Act to provide the FDA with performance goals for premarket reviews and to establish user fees for manufacturers submitting filings to the FDA.[51] "In enacting MDUFMA, Congress recognized that 'the public health will be served' by providing additional funds to FDA for 'the process for the review of devices and the assurance of device safety and effectiveness so that statutorily mandated deadlines may be met.'"[52] For fiscal year 2024, the cost of a 510(k) notification is $24,335, while a PMA application costs $540,783.[53] The cost to supplement an approved PMA for modification of or general improvement to the existing device ranges from $8,653 to change facility for manufacturing, processing, or packaging the device, to $432,626 for significant changes to the device's design, performance, or indication for use.[54] According to FDA performance metrics for original PMA applications and for PMA supplements requesting significant changes received between 2023–2027, the average time to decision was

47. PMA Supplements, 21 C.F.R. § 814.39 (2024); When a Premarket Notification Submission Is Required, 21 C.F.R. § 807.81 (2024).

48. U.S. FOOD & DRUG ADMIN., DECIDING WHEN TO SUBMIT A 510(K) FOR A CHANGE TO AN EXISTING DEVICE: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 41 (2017).

49. *Medical Device Coordination Group*, *Guidance on Cybersecurity for Medical Devices*, at 12, MDCG 2019-16 rev. 1 (2019).

50. U.S. FOOD & DRUG ADMIN., MODIFICATIONS TO DEVICES SUBJECT TO PREMARKET APPROVAL (PMA) – THE PMA SUPPLEMENT DECISION-MAKING PROCESS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 8 (2008).

51. Medical Device User Fee and Modernization Act of 2002, Pub. L. No. 107-250, 116 Stat. 1588.

52. *Summary of the Medical Device User Fee and Modernization Act of 2002*, U.S. FOOD & DRUG ADMIN. (July 8, 2019), https://www.fda.gov/industry/medical-device-user-fee-amendments-mdufa/summary-medical-device-user-fee-and-modernization-act-2002; *see* Medical Device User Fee and Modernization Act § 101.

53. *Medical Device User Fee Amendments (MDUFA): Fees*, U.S. FOOD & DRUG ADMIN. (Sep. 3, 2025), https://www.fda.gov/industry/fda-user-fee-programs/medical-device-user-fee-amendments-mdufa.

54. *Id.*

290 calendar days.[55] In contrast, the FDA's average time to decision for 510(k) notifications was only 128 calendar days.[56] This complex, costly, and time-consuming regulatory regime only covers the United States.

2. Regulation Outside of the United States

Manufacturers identify target markets for their devices based on factors such as market size, growth potential, competition, adequate reimbursement policies for the device, and costs associated with entering the regulatory environment.[57] Before manufacturers can bring their devices to market, they must adhere to that nation's regulatory requirements. Although global medical device regulations are designed primarily to ensure safety, each country has a unique framework that must be satisfied before the regulatory agency will approve the device for distribution in its country.[58] Beyond seeking the FDA's nod of approval, companies may seek to obtain Chinese National Medical Products Administration (NMPA) medical device approval; approval from Brazil's Agência Nacional de Vigilância Sanitária (ANVISA); approval from Japan's Pharmaceuticals and Medical Devices Agency (PMDA) and Ministry of Health, Labour and Welfare (MHLW); a device license from Health Canada; or CE mark, which is the requirement to distribute medical products in Europe.

The European medical device market is the second largest market behind the United States.[59] Not only has Europe embarked on a new data strategy, but the European Commission also introduced a major update to the medical device regulations in 2017, changing the landscape for medical device compliance in Europe. The Medical Device Regulation (Regulation (EU) 2017/745, hereinafter referred to as the MDR) replaced the previous Medical Device Directive (MDD, Council Directive 93/42/EEC) to strengthen protection against risks posed by medical devices.[60] The new regulation increased focus on device safety and updated regulations to properly account for new technologies by: (1) introducing more stringent clinical evidence requirements, (2) strengthening post-market surveillance requirements, (3) enhancing traceability by requiring medical devices to carry a Unique Device Identification (UDI) code, and (4) requiring manufacturers to demonstrate compliance with the most recent and advanced stage of

55. *MDUFA Performance Goals and Procedures, Fiscal Years 2023 Through 2027*, U.S. FOOD & DRUG ADMIN. 2, https://www.fda.gov/media/158308/download (last visited Mar. 10, 2026).

56. *Id.*

57. *Regulatory Strategy: A Comprehensive Guide to Navigating the Global Market*, NSF (June 24, 2024), https://www.nsf.org/knowledge-library/regulatory-strategy-comprehensive-guide-navigating-global-market.

58. Chettri & Ravi, *supra* note 21, at 468.

59. James Cunningham et al., *Medical Device Sectoral Overview*, WHITAKER INST. 9 (2015); *see also* Sujan Rajbhandary & J. Davis Rolfe, Jr., *2024: Five Trends to Watch in the Medical Device Industry*, MERCER CAP., https://mercercapital.com/article/5-trends-to-watch-in-the-medical-device-industry-2024/ (last visited Mar. 10, 2026) (evaluating factors and trends that influence supply and demand of medical devices, including a comparison of the regulatory regimes in the U.S. and European Union).

60. Wendy Levine, *EU MDR Overview – A Major Update to European Medical Device Regulations*, RIMSYS (Apr. 8, 2022), https://www.rimsys.io/blog/eu-mdr-overview.

technical development (referred to within the MDR as "State Of The Art" (SOTA)).[61]

Regardless of which market a manufacturer registers its medical device in, medical devices are continually modified over time; furthermore, regulatory agencies have long mandated that medical device manufacturers maintain a formal and systematic approach to manage, control, and evaluate all changes to their products or processes to determine the extent to which the safety and effectiveness of their devices are impacted.[62] Medical device manufacturers face strong headwinds due to complex registration frameworks that vary by country. Each of the regulatory frameworks is fraught with its own challenges, including both substantive and financial challenges from submission costs, as countries differ in the aims of regulation and the process involved.[63] For example, countries' change management processes and requirements vary for device and process modifications, prompting manufacturers to view and treat proposed changes differently.[64] A change that does not require a new FDA submission might need a full review in the EU according to EU MDR, and so on.[65] Considering these challenges, device manufacturers may understandably opt to avoid investing in projects that require filings, causing patients to pay the price.

B. Software in Medical Devices

Unsurprisingly, the medical device industry—like so many aspects of daily life—has embraced the digital revolution. Many of today's medical devices are operated by microprocessors, and most of their functions are dictated through internal software.[66] Software can be either (1) stand-alone used in a medical environment, (2) integral to a medical device, or (3) used in manufacture or maintenance of a medical device.[67] Software integral to a medical device is software that is embedded in the device such that the device cannot perform its primary function without it.[68] This type of embedded software is also considered a medical device

61. *EU MDR Overview: An Update to European Medical Device Regulations*, REGDESK (Apr. 6, 2023), https://www.regdesk.co/eu-mdr-overview-an-update-to-european-medical-device-regulations/; *MDCG Guidance on Standardisation for Medical Devices: Harmonised Standards*, REGDESK (Sep. 3, 2024), [https://web.archive.org/web/20250218101637/https://www.regdesk.co/mdcg-guidance-on-standardisation-for-medical-devices-harmonised-standards/].

62. *Medical Device Change Management Process Best Practices*, ORIEL (Oct. 22, 2023), https://www.orielstat.com/blog/medical-device-change-control-process/.

63. Sundeep Mishra, *FDA, CE Mark or Something Else?—Thinking Fast and Slow*, 69 INDIAN HEART J. 1, 1 (2017).

64. *Medical Devices Change Management in the European Union and MDSAP Countries*, THEMA, http://www.thema-med.com/en/2024/10/15/la-gestione-delle-modifiche-nei-dispositivi-medici-in-unione-europea-e-nei-paesi-mdsap/ (last visited Mar. 10, 2026).

65. *Id.*

66. Kahn, *supra* note 12, at 93.

67. *Software as a Medical Device (SaMD)*, U.S. FOOD & DRUG ADMIN. (Dec. 4, 2018), https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd.

68. Wendy Levine, *Software as a Medical Device (SAMD) – Classification Overview*, RIMSYS (Feb. 7, 2022), https://www.rimsys.io/blog/software-as-a-medical-device-samd.

and thus subject to FDA regulation based on the quality and safety requirements of its parent device.[69]

The FDA intends to apply its regulatory oversight to only those software functions that are themselves classified as medical devices and whose functionality could pose a risk to patient safety if the device were to not function as intended.[70] The degree of the FDA's regulatory oversight largely depends on the intended use of the software.[71] Some software functions may meet the definition of a medical device, but because they pose a lower risk to the public, the FDA exercises enforcement discretion over these devices.[72] For example, the FDA will focus its regulatory oversight on software functions that are intended to control the operation of the parent device because of the potentially serious effect on the patient's well-being caused by an error in the software.[73] While software that provides behavioral technique or audio messages as part of the user's treatment for diagnosed psychiatric conditions or software that provides periodic educational information to pregnant people may meet the definition of medical device, they pose lower risk to public safety, and thus the FDA intends to exercise enforcement discretion.[74]

The range of possible applications for software in medical devices is extensive, potentially reshaping the way healthcare is delivered, monitored, and managed. Here are a few examples:

- Arrhythmia detectors contain embedded software to monitor an electrocardiogram (ECG) and to produce a visible or audible alarm when an atrial or ventricular arrythmia exists;[75]
- Intravascular ultrasound systems are software-driven systems that "aim[] for exceptional, real-time image guidance and visualization of anatomical structures to help clinicians increase their confidence when performing complex interventional cardiology and electrophysiology procedures;"[76] and
- Surgical robotic systems combine medical science, robotics, and engineering to enhance surgical procedures by improving precision and

69. Bruce Merlin Fried & Jason Mark Zuckerman, *FDA Regulation of Medical Software*, 33 J. HEALTH L. 129 (2000).

70. U.S. FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 2 (2022).

71. Jonathan S. Kahan, *The Evolution of FDA Regulation of New Medical Device Technology and Product Applications*, 41 FOOD DRUG COSM. L.J. 207, 211 (1986).

72. U.S. FOOD & DRUG ADMIN., *supra* note 70.

73. *Id.* at 27-28.

74. *Id.* at 6-7.

75. *Arrhythmia Detector and Alarm – Class II Special Controls Guidance Document for Industry and FDA Staff*, U.S. FOOD & DRUG ADMIN. (July 2, 2018), https://www.fda.gov/medical-devices/guidance-documents-medical-devices-and-radiation-emitting-products/arrhythmia-detector-and-alarm-class-ii-special-controls-guidance-document-industry-and-fda-staff.

76. *FDA Clears GE Healthcare's New Intravascular Ultrasound*, DIAGNOSTIC & INTERVENTIONAL CARDIOLOGY (Oct. 15, 2008), https://www.dicardiology.com/product/fda-clears-ge-healthcares-new-intravascular-ultrasound.

> accuracy, while minimizing complications such as infections, pain, and blood loss.[77]

These examples represent a small fraction of the medical technologies with embedded software that enhance decision-making, reduce medical errors, and contribute to a more efficient and effective healthcare system.

Software that is developed to be incorporated into a medical device is generally comprised of source code that is written in a manner consistent with software industry best practices based on the international standard IEC 62304.[78] Software source code for a medical device may also include Off-The-Shelf (OTS) software components developed outside of the company for purposes other than the specific product application sought by the company.[79] It likely also includes legacy software code components that were previously developed internally either for a different product and reused or for an earlier version of a device.

After market introduction of a medical device containing software, clinical use exposes software defects and limitations resulting in the need for ongoing software maintenance and updates. Medical device software typically has logging and auditing capabilities; however, the software source code identifies the data to be logged and made available for analysis.[80] The overall logging and auditing strategy of medical devices often also supports differentiation among recipients, which in some instances means selecting certain log files for specific purposes. In other instances, this means inclusion or exclusion of information, e.g., de-identification of certain logs when exported from a device.[81] Developers and internal service personnel export log files, either by wired connection or through the cloud, and review the records as part of ongoing monitoring of device health or as part of an investigation after a device event occurred during clinical use. These records may inform the root cause investigation into a defect that will be patched as part of ongoing software updates. IEC 62304 provides a framework for systematically managing ongoing software maintenance and updates with patient safety in mind.[82] As discussed in Section I Subsection A of this Comment, any changes to products, including their software, must be evaluated using a risk-based approach to determine the extent to which the safety and effectiveness of the device is impacted.[83] New supplementary filings requiring the FDA's review and prior

77. Yeisson Rivero-Moreno et al., *Robotic Surgery: A Comprehensive Review of the Literature and Current Trends*, CUREUS, July 2023, at 1, 1.

78. INT'L ELECTROTECHNICAL COMM'N, *Foreword* to IEC 62304:2006: MEDICAL DEVICE SOFTWARE – SOFTWARE LIFE-CYCLE PROCESSES (2006), Int'l Standards Org. (defining lifecycle requirements for medical device software).

79. *See* U.S. FOOD & DRUG ADMIN., OFF-THE-SHELF SOFTWARE USE IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (2023).

80. Paul Koster, *Security Analytics and Monitoring of Medical Devices, in* CYBER-PHYSICAL THREAT INTELLIGENCE FOR CRITICAL INFRASTRUCTURES SECURITY 375, 382 (John Soldatos, Isabel Praça, & Aleksandar Jovanović eds., 2021).

81. *Id.*

82. *An In-Depth Guide to IEC 62304: Software Lifecycle Processes for Medical Devices*, JAMA SOFTWARE (Jan. 25, 2024), https://www.jamasoftware.com/blog/an-in-depth-guide-to-iec-62304-software-lifecycle-processes-for-medical-devices.

83. *See* U.S. FOOD & DRUG ADMIN., *supra* note 48, at 7, 41.

approval may be required before the company can release a new software version.[84] Companies may opt to implement software patches that are less substantial rather than making major changes to the software source code to avoid the significant submission costs, high data burden, and lengthy review time associated with the supplementary filings required before software release.

Regulators have expressed concerns with the heightened risk of cyberattack associated with long-lasting medical devices containing outdated legacy software that no longer receive manufacturer support for patches or updates.[85] Although the parent device itself works fine, software made decades ago will be quite different compared to today's modern software.[86] Despite the stricter medical device cybersecurity requirements codified by Congress in the 2023 Consolidated Appropriations Act, which created the new section 524B, "Ensuring Cybersecurity of Devices," in the FD&C Act,[87] there are still challenges to overcome for older medical devices with unsupported, or soon-to-be unsupported, software. Outdated technology and compatibility issues may prevent manufacturers from continuing to issue software patches resulting in unpatched vulnerabilities.[88] These vulnerabilities in internet-connected devices are constantly discovered and can potentially be exploited by malicious actors to gain access to the devices.[89] By exploiting flaws in medical devices, hackers could gain access to the networks to which the devices connect, steal sensitive data, or alter the functionality of the devices themselves and put patient safety at risk.[90]

Removing devices posing a great risk of cyberattack from the market could have serious implications for patient safety and clinical operations.[91] However, the requirement for renewed FDA approval when any changes are made to a medical device, including the embedded software, means additional cost and time to market. This leaves known vulnerabilities open longer than would otherwise occur and likely contributes to the cycle of maintaining legacy source code.[92]

---

84. *Id.* at 12; *PMA Supplements and Amendments*, U.S. FOOD & DRUG ADMIN. (Dec. 12, 2019), https://www.fda.gov/medical-devices/premarket-approval-pma/pma-supplements-and-amendments.

85. Elise Reuter, *Legacy Medical Devices Keep Regulators Up at Night*, MEDTECHDIVE (Oct. 17, 2024), https://www.medtechdive.com/news/legacy-medical-devices-cybersecurity-fda/730114/.

86. Matt Beltz, *The Risk of Using Legacy Medical Devices with Outdated Software*, THE REFINERY (Sep. 16, 2022), https://the-refinery.io/blog/the-risk-of-using-legacy-medical-devices-with-outdated-software.

87. Consolidated Appropriations Act of 2023, Pub. L. No. 117-328, § 524B, 136 Stat. 4459, 5832-34; *Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)*, U.S. FOOD & DRUG ADMIN. (June 26, 2025), https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs.

88. Steve Alder, *FDA Releases Guidance on Managing Legacy Medical Device Cybersecurity Risks*, THE HIPAA J. (Nov. 17, 2023), https://www.hipaajournal.com/fda-guidance-managing-legacy-medical-device-cybersecurity-risks/.

89. Steve Alder, *Riskiest Connected Medical Devices Revealed*, THE HIPAA J. (Apr. 24, 2023), https://www.hipaajournal.com/riskiest-connected-medical-devices-revealed/.

90. *Id.*

91. Alder, *supra* note 88.

92. Patricia A.H. Williams & Andrew J. Woodward, *Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem*, 8 MED. DEVICES: EVIDENCE & RSCH. 305, 312 (2015).

C. Privacy and Data Regulation Predating GDPR and the Big Five

Any company working transnationally is required to comply not only with the medical device laws and regulations of each jurisdiction in which the company either conducts business or utilizes its citizens' data, but also with the corresponding data and privacy regulations in those countries.[93] While the EU's GDPR has placed a spotlight on the issue of data privacy and protection of personal information, the United States already had a complex privacy framework in place with rules that varied by industry and by state.[94] In the midst of the rapid evolution of health information systems, the United States Congress recognized the need for a system to protect patients' sensitive medical records and health information and enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996.[95] HIPAA created national standards to protect sensitive patient health information from disclosure without the patient's consent or knowledge.[96]

1. HIPAA and the Privacy Rule

One prominent feature of HIPAA is the Privacy Rule. HIPAA's Privacy Rule "forbids an organization subject to its requirements (a 'covered entity') from using or disclosing an individual's health information ("protected health information" [or PHI]) except as mandated or permitted by its provisions."[97] "An entity violates HIPAA by obtaining or disclosing a person's identifiable health information without authorization."[98] "Covered entities" include health care providers, health plans, health care clearinghouses, and health care providers that handle PHI.[99] "'Providers' include all entities that provide health related services as well as products, and specifically include pharmacists and durable medical equipment providers."[100]

> "Protected health information" is any individually identifiable information concerning the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for that provision of health care to an individual.[101]

---

93. Fujimori-Smith, *supra* note 4, at 91.

94. Jacob Nix & Pascal A. Bizarro, *US Data Privacy Law: A Disparate Landscape in Need of Consolidation*, 5 ISACA J. 1, 1 (2020).

95. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

96. State v. Cusson, 269 A.3d 828, 843 n.18 (Conn. App. 2022).

97. Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 43 n.15 (2014) (quoting Arons v. Jutkowitz, 9 N.Y.3d 393, 412-13 (2007)).

98. Hall v. St. Jude Med. S.C., Inc., 326 F. Supp. 3d 770, 783 (D. Minn. 2018).

99. Applicability, 45 C.F.R. § 160.102(a)(1) (2000).

100. Diane Kutzko et al., *HIPAA in Real Time: Practical Implications of the Federal Privacy Rule*, 51 DRAKE L. REV. 403, 412 (2003).

101. *Id.* at 411.

The main identifiers that qualify as PHI include: names, telephone numbers, email addresses, Internet Protocol (IP) addresses, geographic data, license numbers, biometric identifiers, or any unique identifying code or number.[102] The Privacy Rule introduces the "minimum necessary" principle, which requires a covered entity to "make reasonable efforts" to limit disclosure of PHI to the minimum necessary to accomplish both internal intended purposes.[103]

To reduce risks to individuals and support the secondary use of data for comparative effectiveness studies, policy assessment, life sciences research, and other endeavors, HIPAA's Privacy Rule permits a covered entity or its business associates to create information that is not individually identifiable through a de-identification process.[104] The Privacy Rule provides two de-identification methods: (1) a formal determination by a qualified expert, or (2) the removal of eighteen specified individual identifiers, combined with the absence of actual knowledge or awareness by the covered entity that the information is not actually de-identified so it could be used to identify the individual who is the subject of the information.[105] While de-identification may result in loss of information, health data that has been de-identified in accordance with Section 164.514(a) of the HIPAA Privacy Rule is no longer covered by the Rule, as it no longer meets the criteria for PHI.[106]

Companies developing medical devices and software are considered covered entities whose compliance with HIPAA involves adhering to stringent standards and guidelines to safeguard the confidentiality, integrity, and availability of patient health information within their products and services.[107] Beginning in the concept stage, medtech companies must integrate HIPAA-compliance considerations into the planning and design of their products.[108] This involves conducting thorough risk assessments to identify potential privacy and security vulnerabilities, as well as implementing appropriate safeguards to mitigate these risks.[109] After market introduction, companies must monitor and regularly maintain their software to address emerging security threats and ensure continued compliance with evolving HIPAA regulations.[110]

In practice, potential areas of liability for non-compliance that medtech companies face include the functionalities of the software embedded in the medical

---

102. *Guidance on HIPAA Compliance for Medical Devices*, SIERRA LABS (Sep. 17, 2020, at 08:38 ET), https://blog.sierralabs.com/guidance-on-hipaa-compliance-for-medical-devices.

103. Kutzko et al., *supra* note 100, at 414.

104. *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Feb. 3, 2025), https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html (citing Uses and Disclosures of Protected Health Information: General Rules, 45 C.F.R. § 164.514(a)-(b) (2024)).

105. *Id.*

106. *Id.*

107. Sara Seitz, *HIPAA and the Development of MedTech Software*, SEQUENEX (Apr. 25, 2024), https://sequenex.com/hipaa-and-the-development-of-medtech-software/.

108. *Id.*

109. *Id.*

110. *Id.*

devices themselves, service records containing software log files, medical device and healthcare advertising and promotional materials, and case study presentations by physicians. Medical device software that stores, analyzes, and transmits patient data, including during the provision of ongoing preventative maintenance and servicing of the device, needs to be specially designed to be compliant with data privacy regulations of each country in which the company intends to conduct business or otherwise utilizes that country's citizens' data. Software source code should be written in a way to handle information such that data is only flowing from the patient to authorized parties; and, if a device is receiving information, it can only do so with the patient's consent.[111] If the software does receive and retain PHI, the logging and auditing strategy of the device should support exclusion of protected information through de-identification of logs when exported from a device.[112]

The HIPAA Privacy Rule provides companies with clear guidance on the requirements for de-identifying PHI, as discussed previously.[113] As an additional measure of protection, companies should implement security protocols that encrypt incoming and outgoing data. Advertising, promotional materials, and case study presentations often include summaries from the clinical use of medical devices and should be reviewed for any personally identifiable information.

II. GDPR AND IMPACT OF EU'S DATA LEGISLATION ON DEVICE INNOVATION

In February 2020, the European Commission published the European Data Strategy, which is a policy program that aims to create "a society empowered by data" and to build "a strong legal framework—in terms of data protection, fundamental rights, safety and cybersecurity."[114] Through the data strategy, the Europe Commission sought to promote Europe's competitiveness and establish Europe as a global leader in a data-driven society.[115] The European Commission balanced the flow and various uses of data, while preserving privacy, security, safety, and ethical standards.[116] Flowing from the data strategy were the Big Five

111. Kayla Matthews, *Medical Devices and HIPAA Compliance: What to Know*, HEALTHIT ANSWERS (Nov. 13, 2019), https://www.healthitanswers.net/medical-devices-and-hipaa-compliance-what-to-know/.

112. Koster, *supra* note 80, at 382.

113. *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, *supra* note 104.

114. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, at 1, COM (2020) 66 (Feb. 19, 2020).

115. Tobias Bräutigam et al., *EU Regulation Builds a Fairer Data Economy – The Opportunities of the Big Five Proposals for Businesses, Individuals and the Public Sector* 14 (Sitra, published working paper, 2022), https://www.sitra.fi/app/uploads/2022/06/sitra-eu-regulation-builds-a-fairer-data-economy.pdf.

116. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, *supra* note 114, at 1.

data legislation—the Data Act,[117] the Artificial Intelligence (AI) Act,[118] the Data Governance Act,[119] the Digital Markets Act,[120] and the Digital Services Act[121]—enacted alongside the GDPR,[122] which is another key legal instrument relating to the data economy.

A. The Big Five Data Legislation

The Data and AI Acts are of the most relevance to the medical device industry. The Data Act, which expressly mentions medical and health devices,[123] provides new substantive rights on all data—specifically, who is entitled to access or control non-personal data—to promote opportunities for data-driven innovation.[124] "Any connected…device or wearable that obtains, generates, or collects data of the person using [it] or their environment will be under the scope of the Data Act."[125] Through the AI Act, the European Commission aimed to enact the first global regulation specifically targeting AI.[126] The purpose of this Act is to increase trust in AI-enabled technologies and ensure that AI systems used within the EU are safe, transparent, traceable, non-discriminatory, environmentally friendly, and overseen by people, rather than by computer automation using algorithms alone, to prevent harmful outcomes.[127] Medical technologies, including medical device software, may come under the scope of the AI Act. Some requirements under the AI Act are new for the medtech sector (e.g., data governance, human oversight, accessibility requirements), and thus required medical device manufacturers to undertake additional training and update internal procedures and technical documentation to ensure compliance.[128]

The remaining pieces of Big Five legislation are less impactful to medical device companies. The Data Governance Act is the framework for data access and

117. Council Regulation 2023/2854 (Data Act), which became law on Dec. 13, 2023, and became applicable in Sep. 2025. 2023 O.J. (L 2854) 71 (EU).

118. Council Regulation 2024/1689 of the European Parliament and of the Council of June 13, 2024, 2024 O.J. (L 1689) 123 (EU) (showing application of rules on high-risk AI systems under Annex I of the AIA is required by Aug. 2, 2027).

119. Council Regulation 2022/868 of May 30, 2022. 2022 O.J. (L 152) 1 (EU).

120. Council Regulation 2022/1925 of Sep. 14, 2022. 2022 O.J. (L 265) 1 (EU).

121. Council Regulation 2022/2065 of Oct. 19, 2022. 2022 O.J. (L 277) 1 (EU).

122. Council Regulation 2016/679 of Apr. 27, 2016. 2016 O.J. (L 119) 1 (EU).

123. Council Regulation 2023/2854 of Dec. 13, 2023, Recital 14. 2023 O.J. (L 2854) 4 (EU).

124. Bräutigam et al., *supra* note 115, at 17.

125. Gállego et al., *EU Data Act Series (Part 3): Medical and Health Devices and Data Sharing Obligations*, HOGAN LOVELLS (Feb. 28, 2023), https://www.engage.hoganlovells.com/knowledgeservices/news/eu-data-act-series-part-3-medical-and-health-devices-and-data-sharing-obligations.

126. Boland et al., *Implications of the EU AI Act on Medtech Companies*, HOGAN LOVELLS (July 16, 2024), https://www.engage.hoganlovells.com/knowledgeservices/news/implications-of-the-eu-ai-act-on-medtech-companies_1.

127. *EU AI Act: First Regulation on Artificial Intelligence*, EUR. PARLIAMENT: TOPICS (Feb. 19, 2025), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

128. Boland et al., *supra* note 126.

sharing, promoting the availability of data across different sectors and areas.[129] Public sector bodies, data intermediation services, and non-profit data altruism organizations are the entities most impacted by the Data Governance Act.[130] The Digital Markets Act regulates large digital platforms providing core platform services, known as "gatekeepers," by imposing specific obligations on them to promote a fairer business environment.[131] This regulation primarily impacts large tech companies including, but not limited to, Amazon, Apple, Meta, and Microsoft.[132] Finally, the Digital Services Act regulates behavior and content online by creating responsibilities and obligations for different service providers based on their role, size, and impact on the online ecosystem.[133] Online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms are impacted by this regulation.[134]

The new European legislation since 2018, including the transition from the Medical Device Directive to the Medical Device Regulation and the new privacy and data protection legislation, makes clear the strategy for many global medical device companies: pursuing regulatory approval of a new medical device in Europe first has lost its appeal.[135] Previously, companies commonly brought new medical devices to the European market first, since obtaining a CE mark was faster, cheaper, and more predictable than getting regulatory approval elsewhere.[136] Now, MDR has added complexities and unpredictability to the regulatory landscape in Europe and has slowed the pace of medical device innovation in the EU.[137] Coupled with Europe's extensive GDPR and the Big Five data legislation, technological innovation is likely to lag further.

B. General Data Protection Regulation (GDPR)

Europe's data privacy and security law, GDPR, includes new requirements that are setting a high global standard for data protection.[138] This regulation

129. Bräutigam et al., *supra* note 115, at 17.

130. *Data Governance Act Explained*, EUR. COMM'N (Oct. 11, 2024), https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.

131. *The Digital Markets Act: Ensuring Fair and Open Digital Markets*, EUR. COMM'N, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (last visited Mar. 10, 2026).

132. *Id.*

133. Bräutigam et al., *supra* note 115, at 17.

134. *The Digital Services Act: Ensuring a Safe and Accountable Online Environment*, EUR. COMM'N, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en (last visited Mar. 10, 2026).

135. Amanda Pedersen, *Gone Are the Days of Europe-First Medical Device Innovation*, MED. DEVICE & DIAGNOSTIC INDUS. (Mar. 23, 2022), https://www.mddionline.com/regulatory-quality/gone-are-the-days-of-europe-first-medical-device-innovation.

136. *Id.*

137. Christian Johnson et al., *For Cutting-Edge Innovations, the US Pulls Ahead of the EU in Medtech Regulation*, BOS. CONSULTING GRP. (Mar. 11, 2022), https://www.bcg.com/publications/2022/us-ahead-in-medtech-regulation.

138. Bräutigam et al., *supra* note 115, at 28.

provides a single framework that applies in all member states of the European Economic Area (EEA), and it imposes obligations on companies operating around the world, irrespective of location and sector, "so long as they target or collect data related to people in the EU."[139]

The GDPR "itself is large, far-reaching, and…light on specifics, making…compliance a daunting prospect."[140] GDPR requires that: (1) any processing of personal data should be lawful, fair, and transparent; (2) personal data can only be collected and processed for specified, explicit, and legitimate purposes; and (3) personal data collected for one purpose should never be used for a new, incompatible purpose.[141] Personal data collected should be "adequate, relevant and limited to what is necessary for the purposes for which [those data] are processed."[142]

"Unlike HIPAA, which is specifically tailored to [protected] health information, GDPR covers a much broader range of personal data" not limited to just health information.[143] "Personal data" under the GDPR includes any information related to an identified or identifiable data subject (i.e., an individual person) "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."[144] Data can be considered personal if the entity collecting the data in question "has the legal means which enable it to identify the data subject with additional data which the [entity] has about that person."[145] The GDPR further clarifies that personal data concerning health includes "all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject."[146] This includes any information on "a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source."[147] Data ceases to be personal only when it is appropriately anonymized or aggregated so that it can no longer be associated with an identifiable individual.[148]

Data that has been appropriately anonymized is no longer subject to the GDPR, making fully anonymized data "the holy grail of data protection" as it signifies the ultimate goal of privacy.[149] Full anonymization of data irreversibly

139. Wolford, *supra* note 5.

140. *Id.*

141. Council Regulation 2016/679, *supra* note 122, at 7.

142. *Id.*

143. Natalie Calderon, *HIPAA vs. GDPR Compliance: What's the Difference*, MEDSTACK (Oct. 18, 2023), https://medstack.co/blog/hipaa-vs-gdpr/.

144. Council Regulation 2016/679, art. 4(1), *supra* note 122, at 33.

145. *See* Case C-582/14, Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, ¶¶ 49, 65 (Oct. 19, 2016).

146. Council Regulation 2016/679, Recital 35, *supra* note 122, at 6.

147. *Id.*

148. Council Regulation 2016/679, Recital 26, *supra* note 122, at 5.

149. Andrew Burt et al., *A Guide to the EU's Unclear Anonymization Standards*, IAPP (July 15, 2021), https://iapp.org/news/a/a-guide-to-the-eus-unclear-anonymization-standards.

prevents the identification of the individual to whom it relates.[150] Therefore, fully anonymized data is the ideal state in which data can be used without any restrictions related to data protection laws because no individual can be identified from it.[151] However, it is nearly impossible to perfectly and fully anonymize data, as some possibility of reidentification often remains.[152] The main problem that companies face when incorporating the GDPR data protection requirements and principles into their processes and the design of their products is the significant uncertainty around what appropriate "anonymization" means in practice.[153]

One alternative to entirely anonymizing data is to consider all deidentified data as pseudonymized. "Pseudonymization" is a data security measure recommended in GDPR and is defined in the regulation as:

> the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[154]

While pseudonymized data does not fall outside the scope of EU data protections because reidentification is still possible, the compliance burden on pseudonymous data can be significantly lighter since identifying characteristics of data have been replaced with a pseudonym, prohibiting the data subject to be directly identified—meaning that the data can no longer be attributed to a specific data subject without the use of additional information.[155] Nevertheless, pseudonymized data remains in the purview of the GDPR, as pseudonymization only provides limited protection for the identify of data subjects as it is technically reversible and allows identification indirectly by analysis of the underlying data.[156] GDPR encourages companies to safeguard privacy and data protection principles from the start by implementing technical and organizational measures, such as minimizing the processing of personal data and pseudonymizing personal data that is processed, at the earliest stages of the lifecycle of the device or software development.[157] While there are a host of options companies can use to get the value out of their data while ensuring it remains protected, there is no one-size-fits-all approach to

150. *Guidance Note: Guidance on Anonymisation and Pseudonymisation*, DATA PROT. COMM'N 2 (June 2019), https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf.

151. *Id.* at 3.

152. Burt et al., *supra* note 149.

153. *Id.*

154. Council Regulation 2016/679, art. 4(5), *supra* note 122, at 33.

155. *Guidance Note: Guidance on Anonymisation and Pseudonymisation*, *supra* note 150, at 3.

156. *Id.*

157. *What Does Data Protection 'By Design' and 'By Default' Mean?*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (last visited Mar. 10, 2026).

anonymization and companies are forced to select an approach despite the ambiguity that persists.[158]

Compliance costs are high, and fines for failing to comply with GDPR can be astronomical.[159] Unlike HIPAA, which has a maximum fine of $1.5 million annually,[160] failure to comply with GDPR may result in "a reprimand, a temporary or definitive ban on processing and a fine of up to €20 million or 4% of the business's total annual worldwide turnover."[161] Violators of the GDPR's privacy and security standards have faced harsh fines, with penalties totaling tens of millions of euros plus damages sought by data subjects.[162] Data Protection Authorities (DPAs) are independent public authorities that supervise the application of GDPR and have investigative and corrective powers.[163] When investigating a case of non-compliance and determining appropriate enforcement action, DPAs consider a number of factors such as "the nature, gravity and duration of the infringement, its intentional or negligent character, any action taken to mitigate the damage suffered by individuals, [and] the degree of cooperation of the organization."[164] DPAs can issue warnings or reprimands when processing operations that violate GDPR's requirements and order companies to comply with a data subject's request to exercise her rights over her personal data. These rights include the rights of access, to rectification, to erasure, to restrict processing, to data portability, to object, and to not be subject to a decision based solely on automated processing.[165] DPAs can also order companies to communicate after a personal data breach or ban processing and have the authority to impose administrative fines.[166] When imposing fines for non-compliance, DPAs ensure

158. Burt et al., *supra* note 149.

159. *See What if My Company/Organisation Fails to Comply with the Data Protection Rules?*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_en (last visited Mar. 10, 2026).

160. *What Are the Penalties for HIPAA Violations?*, THE HIPAA J., https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations (last visited Mar. 10, 2026); *HIPAA Violations & Enforcement*, AM. MED. ASS'N, https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement (last visited Mar. 10, 2026); Edemekong et al., *Health Insurance Portability and Accountability Act (HIPAA) Compliance*, NAT'L LIBR. OF MED. (Nov. 24, 2024), https://www.ncbi.nlm.nih.gov/books/NBK500019/#:~:text=Civil%20violations&text=For%20a%20HIPAA%20violation%20due,or%20$1.5%20million%20per%20violation.

161. *What if My Company/Organisation Fails to Comply with the Data Protection Rules?*, *supra* note 159.

162. Wolford, *supra* note 5.

163. *Legal Framework of EU Data Protection*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en (last visited Mar. 10, 2026).

164. *What if My Company/Organisation Fails to Comply with the Data Protection Rules?*, *supra* note 159.

165. *See Rights of the Individual*, EUR. DATA PROT. SUPERVISOR, https://www.edps.europa.eu/data-protection/our-work/subjects/rights-individual_en (last visited Mar. 10, 2026).

166. *Data Protection Authority & You*, EUR. DATA PROT. BD.: DATA PROT. GUIDE FOR SMALL BUS., https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en#:~:text=Reprimands:%20in%20the%20case%20of,became%20aware%20of%20the%20issue (last visited Mar. 10, 2026).

that the penalty fee imposed in each individual case is "effective, proportionate and dissuasive."[167]

Since GDPR went into effect on May 25, 2018, the primary focus of enforcement by DPAs for breaches of data protection have related to "lawful processing" and "transparency of data processing."[168] The top fines imposed for GDPR violations were imposed on U.S.-based technology giants Meta and Amazon.[169] U.S.-based medical device and medtech companies have not escaped DPA enforcement. The Italian DPA imposed a fine of €300,000 on Medtronic, an American-Irish medtech company that develops, manufactures, and sells medical devices and therapies for treatment of over seventy health conditions,[170] for non-compliance with general data processing principles.[171] Specifically, Medtronic sent emails to hundreds of people using their medical device, inadvertently making the email addresses of recipients visible to the other recipients.[172] Additionally, Argon Medical Devices, an American company offering medical devices for interventional radiology, oncology, and vascular surgery procedures, was fined €220,000 by the Norwegian Supervisory Authority for failing to report a security breach that affected the personal data of all their European employees.[173]

III. THE FUTURE OF MEDICAL DEVICE INNOVATION

Despite the EU's ambitious agenda to shape the global digital landscape through enactment of the GDPR and the Big Five data and privacy legislation, the medical device industry remains skeptical about implementation of the new requirements given the uncertainty and ambiguity in the laws and the high associated costs for compliance. The GDPR brings personal data into a complex regulatory regime with profound implications.[174] Companies have publicized their

---

167. *What if My Company/Organisation Fails to Comply with the Data Protection Rules?*, *supra* note 159.

168. Brian Daigle & Mahnaz Khan, *One Year In: GDPR Fines and Investigations Against U.S.-Based Firms*, U.S. INT'L TRADE COMM'N (Sep. 2019), https://www.usitc.gov/publications/332/executive_briefings/gdpr_enforcement.pdf.

169. Meta was fined $1.3 billion USD after an Irish court ruled that it violated GDPR laws related to data transfers between the EU and the US. The second biggest GDPR fine to date was $781 million USD imposed on Amazon by Luxembourg's National Commission for Data Protection (CNPD) for not getting consent from its users before storing advertisement cookies. Osman Husain, *52 Biggest GDPR Fines and Penalties (2018 – 2024)*, ENZUZO (July 23, 2024), https://www.enzuzo.com/blog/biggest-gdpr-fines.

170. *See Our Global Presence*, MEDTRONIC, https://www.medtronic.com/en-us/our-company/locations.html (last visited Mar. 10, 2026).

171. Medtronic was fined for violation of GDPR Art. 5(1)(a), (f), Art. 9, Art. 12, Art. 13, and Art. 32 for non-compliance with general data processing principles. *Details Page for ETid-2245*, CMS: GDPR ENF'T TRACKER, https://www.enforcementtracker.com/ETid-2245 (last visited Mar. 10, 2026).

172. *Id.*

173. Argon Medical Devices was fined for violation of GDPR Art. 33 (1) for insufficient fulfilment of data breach notification obligations. *Details Page for ETid-1697*, CMS: GDPR ENF'T TRACKER, https://www.enforcementtracker.com/ETid-1697 (last visited Mar. 10, 2026).

174. Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'NS TECH. L. 65, 66 (2019).

concerns about the adverse effect that compliance with the new onerous data protection rules imposed by GDPR may have on their business, financial condition, or results of operation, due to the additional costs for compliance and significant increase in overall risk exposure.[175] In one instance, Stryker, an American multinational medical technology company that makes products and services in the areas of medical-surgical, neurotechnology, and orthopedics, stated the following in its annual report for the fiscal year ending December 31, 2023, concerning the legal and regulatory risks associated with privacy and data security regulations such as EU's GDPR:

> These laws and regulations are broad in scope and are subject to evolving interpretation and we have in the past been, and in the future could be, required to incur substantial costs to monitor compliance or to alter our practices. As new privacy-related laws and regulations are implemented, the time and resources needed for us to comply with such laws and regulations, as well as our potential liability for non-compliance and reporting obligations in the case of data breaches, have increased and may further increase.[176]

Companies that do business in the EU, or handle the personal data of EU residents and thus fall within the scope of GDPR, are faced with the need to recalibrate their policies by embedding strong privacy standards into their operations, not only to comply with the regulation, but also to create an environment of trust with consumers and regulators.[177] Under GDPR, companies can no longer bury data collection policies deep in legalistic "terms and conditions" that are often overlooked.[178] Instead, they must ensure that their processes minimize impact on individuals' privacy rights.[179] Recognizing the necessity of a Data Protection Officer (DPO) is a crucial first step in GDPR compliance.[180] A DPO is required under GDPR if the company's "core activities involve processing of sensitive data on a large scale or involve large scale, regular and systematic monitoring of individuals."[181] Companies should consider appointing someone in the EU as a liaison with regulators, and GDPR requires

175. *See* SEC. & EXCH. COMM'N, FORM 10-K: INTUITIVE SURGICAL, INC. (2025); SEC. & EXCH. COMM'N, FROM 10-K: BOS. SCI. CORP. (2024).

176. SEC. & EXH. COMM'N, FORM 10-K: STRYKER CORP. (2024).

177. Rey LeClerc Sveinsson, *GDPR Compliance Checklist: A Guide for U.S. Companies*, ERMPROTECT, https://ermprotect.com/blog/gdpr-compliance-checklist-a-guide-for-us-companies/ (last visited Mar. 10, 2026).

178. Jeremy Kahn et al., *It'll Cost Billions for Companies to Comply with Europe's New Data Law*, BLOOMBERG (Mar. 22, 2018, at 01:01 ET), https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law.

179. *Id.*

180. Sveinsson, *supra* note 177.

181. *Does My Company/Organisation Need to Have a Data Protection Officer (DPO)*?, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/data-protection-officers/does-my-companyorganisation-need-have-data-protection-officer-dpo_en (last visited Mar. 10, 2026).

many larger companies to designate a DPO responsible for compliance and fostering a culture of data protection within the organization.[182]

Next, companies should conduct an audit to identify all personal data that it collects, processes, and stores, along with the purpose for each type of data that is collected and processed, with whom the data is shared, and the method and length of time the data is stored.[183] If this audit leads to the determination that processing operations are likely to result in high risks to the rights and freedoms of natural persons, a Data Protection Impact Assessment (DPIA) is required under GDPR.[184] A DPIA is a process designed to map out the processing operations, assess the necessity and proportionality of the processing, and evaluate risks to the rights and freedoms of data subjects.[185] As a proactive measure, companies should integrate DPIAs into the ongoing risk management process to ensure that all new or previously unassessed risks are managed effectively.[186]

Business operations should be adapted to implement technical and organizational measures that safeguard privacy and data protection from the earliest stages of the design.[187] By embedding such technical and organizational measures in operational processes, companies can ensure that personal data is processed, by default, with the highest privacy protection.[188] Examples of operational processes that should be revisited for compliance with the peculiarities of the GDPR include the way Information Technology (IT) and Human Resources (HR) systems landscapes are designed, the way internal audits are carried out, the way companies contract with vendors and customers, and the way medical devices that contain software retain information captured during clinical use. Each of these areas of business operations may be privy to sensitive and confidential data. To illustrate, IT and HR systems may contain and process large amounts of sensitive personal data on the company's employees, contractors, former employees, and job applicants, including health information, medical records, and salary levels.[189] Similarly, medical devices that contain software may collect some personal information related to the practitioner or the patient during use of the device.[190] Such information could be captured in the device's software log files and may be accessible for export; therefore, safeguarding privacy and data protection should be considered from the early stages of software development.

---

182. Kahn et al., *supra* note 178.

183. Sveinsson, *supra* note 177.

184. *Id.*

185. *Id.*

186. *Id.*

187. This principle is known as "data protection by design." *What Does Data Protection 'By Design' and 'By Default' Mean?*, *supra* note 157.

188. *Id.*

189. Katalin Hadabas, *How Is GDPR Affecting Human Resources Professionals?*, TRESORIT (Sep. 12, 2022), https://tresorit.com/blog/how-will-the-gdpr-affect-human-resources-professionals/.

190. Nuria Gresa et al., *Artificial Intelligence (AI), General Data Protection Regulation (GDPR) and Cybersecurity: 10 Misconceptions About Medical Device Software*, MEDIDEE, https://medidee.com/2022/09/15/artificial-intelligence-ai-general-data-protection-regulation-gdpr-and-cybersecurity-10-misconceptions-about-medical-device-software/ (last visited Mar. 10, 2026).

As previously described in Section I Subsection B, the range of possible applications for software in medical devices is extensive. Medical device software can range from simple interfaces to complex algorithms that drive critical medical decisions.[191] Various examples of clinical uses of software in a medical device follow:

- Some software embedded in medical devices serve the purpose of motor control, position sensing, monitoring status of batteries, and providing feedback to the user related to the motor position and status to the user through LEDs.[192]
- Some software connects the medical device to networks, allowing the device to be operated, configured, monitored, and serviced remotely.[193]
- More advanced software may contain AI and machine learning (ML) algorithms that enables the device to learn from real-world use and improve the device's performance to better assist providers and improve patient care.[194]

In all instances, defining the software's function and purpose within the medical device and determining whether the software stores, transfers, and/or analyzes personal data are critical for implementation of adequate technical controls to keep data secure and ensure people can exercise data protection rights.[195]

Manufacturers of computer-controlled medical devices, software accessories to medical devices, and stand-alone software systems should review their software source code not only to ensure compliance with current software coding standards but also for elements that raise privacy risks. The DPIA process should include an evaluation of any software embedded in any of its devices, including considerations for: (1) what personal data the device could possibly collect and retain; and (2) the method of servicing and exporting software logs against current and future ways to minimize the amount of personal data captured and further secure the data.[196] Software that connects the medical device to networks allowing it to send and receive data to a cloud server should receive special attention, as most cloud servers are not specifically designed to host confidential data or clinical data.[197] If

191. *An In-Depth Guide to IEC 62304: Software Lifecycle Processes for Medical Devices*, *supra* note 82.

192. "Firmware" refers to the embedded software that directly controls the hardware of a medical device. Vadim Struk, *IoT Firmware Development for Connected Medical Devices*, RELEVANT SOFTWARE (Aug. 13, 2024), https://relevant.software/blog/iot-firmware-development/#What_is_IoT_Firmware.

193. Alder, *supra* note 89.

194. *Artificial Intelligence in Software as a Medical Device*, U.S. FOOD & DRUG ADMIN. (Mar. 25, 2025), https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.

195. *See generally* Nicolas Montauban, *7 Key Principles for GDPR Compliance in Software Development*, CODIFIC (June 17, 2022), https://codific.com/gdpr-compliance-software-development/ (delving into the requirements of EU's GDPR and identifying principles for compliance in the software development workflow).

196. Sveinsson, *supra* note 177.

197. Gresa et al., *supra* note 190.

the privacy assessment uncovers a risk that is not appropriately mitigated, operational business processes related to software should be revisited and the source code itself may require updates to enhance data security and mitigate risks. Updates may include pseudonymization to minimize the amount of personal data that is collected, implementing appropriate retention policies, and securely deleting or anonymizing data once it is no longer required.[198]

The tasks companies face to comply with the EU's GDPR, including hiring new privacy professionals and enhancing employee training, developing new privacy policies throughout their organizations, and implementing one-time modifications to processes and products, come with a significant price tag.[199] Ernst & Young, a global professional services firm, reported that the world's 500 biggest corporations expected to spend a total of $7.8 billion to comply with the GDPR during the first year after it went into effect.[200] In 2018, a survey found that companies each forecasted spending more than €1.3 million ($1.4 million) on GDPR readiness initiatives.[201] The economic impact from the cost of compliance is palpable. Companies are unconvinced though that the requirements set forth in the regulation meaningfully reduce the risk of consumer harm, and instead are only check boxes for compliance, serving no valuable business function.[202] Companies are therefore left balancing the costly endeavor of GDPR compliance with the harsh penalties they could face for non-compliance.

CONCLUSION

It is a fundamental European insight that mankind is served best where the channels of commerce flourish.[203] However, the increased regulatory burdens that companies face when attempting to get improved technology to the medical device market has had clear negative consequences on business growth and innovation.[204] EU's GDPR has raised consumer awareness about data privacy and personal data rights, and it has transformed how organizations handle personal data. A company's failure to prioritize data privacy can not only result in significant

198. Sveinsson, *supra* note 177.

199. Nicole Lindsey, *Global 500 Faces GDPR Compliance Costs of $7.8 Billion*, CPO MAG. (Dec. 1, 2017), https://www.cpomagazine.com/data-protection/global-500-faces-gdpr-compliance-costs-of-7-8-billion/.

200. Kahn et al., *supra* note 178.

201. *Veritas Study: Organizations Worldwide Fear Non-compliance with New European Union Data Regulation Could Put Them Out of Business*, VERITAS (Apr. 25, 2017), https://www.veritas.com/news-releases/2017-04-25-veritas-study-organizations-worldwide-fear-non-compliance-with-new-european-union-data-regulation-could-put-them-out-of-business.

202. Daniel Castro, *5 Lessons the U.S. Can Learn from European Privacy Efforts*, GOV'T TECH., (Aug. 2019), https://www.govtech.com/policy/5-lessons-the-us-can-learn-from-european-privacy-efforts.html.

203. Julian Schneider, *The Origins and Future of International Data Privacy Law*, 47 U.C. L. S.F. INT'L L. REV. 1, 21 (2024).

204. Ryan Preston, *Stifling Innovation: How Global Data Protection Regulation Trends Inhibit the Growth of Healthcare Research and Start-Ups*, 37 EMORY INT'L L. REV. 135, 164 (2022).

penalties, but also harm to their reputation in industry and reduce consumer trust.[205] Yet, overly protective data privacy laws in tandem with the pre-existing regulatory regimes for medical devices have proven harmful to health by delaying innovation that could diagnose, treat, and rehabilitate diseases.[206]

GDPR has had an undeniably transformative impact on data protection and privacy laws globally.[207] It has created momentum for lawmakers in the United States and around the world to introduce their own GDPR-inspired proposals for regulating data privacy.[208] Nevertheless, there is still no comprehensive federal law in the U.S. regulating data privacy. Going forward, policymakers should consider the cost and benefits of compliance and balance that with the adverse effect of increased regulation on innovation and the accessibility of valuable medical technologies. Future legislation should avoid rules that could steer companies to focus on checkbox compliance and instead strive to create a national data protection and privacy framework that streamlines regulation without hampering innovation.

205. Tosan Ebisan, *GDPR: Five Years on and What Have We Learned?*, DOTDIGITAL (June 12, 2023), https://dotdigital.com/blog/gdpr-five-years-on-what-have-learned/.

206. Preston, *supra* note 204, at 164.

207. Gabriela Zanfir-Fortuna, *What to Expect in Global Privacy in 2025*, FUTURE OF PRIV. F. (Jan. 23, 2025), https://fpf.org/blog/what-to-expect-in-global-privacy-in-2025/.

208. *Id.*