XI. Data Protection on the Doorstep: How the GDPR Impacts American Financial Institutions

A. Introduction

The General Data Protection Regulation (GDPR, Regulation) became effective on May 25, 2018, immediately impacting any company "offering goods or services" within the European Union (EU).[1] The Regulation responded to the public sentiment that many EU citizens' right to privacy was impinged upon by the proliferation of online data collection and processing.[2] Beginning with the popularization of the internet, personal data became substantially easier to access and track in ways unimaginable in decades prior.[3] Additionally, advanced algorithms now allow utilization of this data in myriad fashions, from predicting social trends to providing personalized financial advice.[4] While processing personal information has many social benefits, the misuse of personal data has the potential to harm individuals.[5] The GDPR attempts to protect individuals from these harms while allowing institutions to continue their beneficial uses of personal data.[6] The GDPR revolutionizes data security for all financial institutions operating within EU member nations and requires compliance with numerous requirements in order to avoid sanctions, increase consumer trust, and maintain successful enterprises.[7]

The most impactful new requirements for financial institutions include the data breach reporting mandate, the heightened client consent requirement, the increased liability for third party vendor

---

[1] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 5.
[2] *Id.* at 1.
[3] *See* ALAN CALDER, *A Brief History of Data Protection, in* EU GDPR A POCKET GUIDE (EUROPEAN) 14 (2016) https://www.jstor.org/stable/j.ctt1m3p1xr (highlighting the growth in availability of computers at the end of the twentieth century).
[4] *See* Regulation 2016/679, *supra* note 1, at 2 (identifying a myriad of technological developments).
[5] *See id.* at 3.
[6] *Id.* at 2.
[7] *See id.*

actions, and the client right to data erasure.[8] To date, no financial institutions have faced sanctions for violations of the GDPR; however, based upon historical EU enforcement data, the first enforcement actions likely will commence in the summer of 2019.[9] Therefore, financial institutions, particularly in the financial technology (Fintech)[10] space, must actively implement and monitor data security plans to prevent possible fines.[11] In contrast to the corporate burdens of the GDPR regulations, the GDPR presents an opportunity for financial institutions by creating uniform standards for data security across Europe[12] and helping institutions prepare for additional forthcoming data protection regulations.[13]

This article begins by analyzing prior EU privacy regulation and the circumstances that led to the passage of the GDPR. Section C examines a provisions from the GDPR that significantly impact financial institutions, including increased consumer consent provisions, stringent data breach requirements, redesigned third-party data processing procedures, and an innovative data portability provision. Section D examines the relevance of the GDPR to U.S.-based financial institutions, speculating on impacts to U.S. institutions operating abroad, and potential impacts that on financial services market

---

[8] Gina Conheady & John Whelan, *EU GDPR: 10 Things Every Fintech Business Should Know*, BLOOMBERG (Aug. 8, 2018, 9:10 AM), https://www.bloomberglaw.com/product/privacy/pds_home/document/XFP8UFMC000000.

[9] *See* Peter Caty, *When Will We Start Seeing GDPR Enforcement Actions? We Guess Feb. 22 2019*, INT'L ASS'N OF PRIVACY PROF'LS (June 28, 2018) https://iapp.org/news/a/when-will-we-start-seeing-gdpr-enforcement-actions-we-guess-feb-22-2019 [https://perma.cc/4XD2-LKN2].

[10] *See* Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 234, 239 (2018) [hereinafter *The Case of Fintech*] (defining Fintech as financial institutions in "the relatively new category of companies whose business models are based on digital products").

[11] *See* Conheady & Whelan, *supra* note 8 (explaining that fintech firms should be especially careful given the large fines imposed by the GDPR and amount of data that these firms process).

[12] *See* Regulation 2016/679, *supra* note 1, at 31 (discussing how EU plans to encourage the free flow of data through regulation at the Union rather than Member State level)

[13] *See* Reece Hirsh & Kristin M. Hadgis, *California's New, GDPR-Like Privacy Law Is a Game-Changer*, BLOOMBERG (July 11, 2018, 7:48 AM), https://www.bloomberglaw.com/product/privacy/document/X6Q3B7MC000000.

competition. Section E article outlines challenges and opportunities that the GDPR presents for these institutions.

B. European Data Privacy Laws and the Passage of the GDPR

The European Parliament and Council enacted the GDPR in response to the dual forces of "the steady march of technological progress" and the inhibition of the free flow of information caused by divergent data privacy regulatory regimes.[14] The technological advances that necessitated revamped data privacy regulation are self-evident to anyone who regularly interfaces with applications on a smartphone.[15] Additionally, an overview of prior European data privacy laws illustrates the resulting flow of information restrictions. Early European privacy laws date back to a 1981 European Council convention aimed at establishing standards for personal data protection while allowing for the flow of information across European nations on computers.[16] As computers and the internet grew in ubiquity, the EU felt the need to update the region's data privacy law by passing the Data Protection Directive (DPD) in 1995.[17] The DPD outlined standards tailored to the prevalence of computers and other electronic devices and the realities of cross-border personal data transfer.[18]

While initially successful, the DPD was not as powerful a tool as the GDPR because of a difference visible in the different legislations' names. That is, the DPD is only a directive, unlike the GDPR, which is a regulation.[19] In EU legislative parlance a directive indicates a set of minimum standards that individual member nations must pass laws to comply with.[20] However, it has no binding authority on individuals or institutions; rather private parties must comply with the

---

[14] CALDER, *supra* note 3, at 16.
[15] *E.g.,* David Grossman, *How Do NASA's Apollo Computers Stack Up to an iPhone?,* POPULAR MECHANICS (Mar. 13, 2017), https://www.popularmechanics.com/space/moon-mars/a25655/nasa-computer-iphone-comparison [https://perma.cc/QE2U-QPY6].
[16] CALDER, *supra* note 3, at 13.
[17] *See id.* at 14.
[18] *See id.*
[19] *See* Regulation 2016/679, *supra* note 1, at 2 (discussing how fragmentation under the DPD resulting from the "differences in the implementation and application of" DPD inhibited the free flow of personal data across borders).
[20] CALDER, *supra* note 3, at 16.

laws passed by each member nation.[21] Conversely, a regulation designates that the enactment is binding law and is enforceable against private parties across the EU from its effective date.[22]

As a directive, the DPD led to a series of varying data privacy laws across Europe.[23] While they were mostly similar, the regulatory structure was too inconsistent for companies to establish a uniform data protection policy that would comply with all EU member nations requirements.[24] Regulatory discord created unequal protections for citizens of different European countries.[25] This, in turn, led to inhibited data transfer across borders, as corporations and regulators were forced to navigate an array of conflicting policies.[26] As a regulation, the GDPR eliminates these regulatory inefficiencies by creating a uniform policy with which institutions can comply while transferring data across the EU.[27] While member nations retain the power to enact more stringent regulations in specific situations,[28] the consistent baseline established by the GDPR should meet the regulation's stated goal of removing fragmentation from data protection within the EU.[29]

---

[21] *Id.*
[22] *Id.*
[23] *See, e.g.*, Loi 17-78 du 6 janvier 1978 de relative à l'informatique, aux fichiers et aux libertés [Law 17-78 of January 4, 1978 on Data Processing, Data Files and Individual Liberties], Journal Officiel de la République Francaise [J.O.] [Official Gazette of France], Jan. 25, 1978; Data Protection Act 1998, c. 29, § 1-75 (Eng.).
[24] *See* Regulation 2016/679, *supra* note 1, at 2 (discussing the problems with the DPD and the need for a consistent regulatory structure across Europe); CALDER, *supra* note 3, at 16.
[25] *See* Regulation 2016/679, *supra* note 1, at 2 (identifying the problems with a fragmented structure of laws).
[26] CALDER, *supra* note 3, at 16 ("[T]he free flow of information was effectively inhibited because the different regulatory environments clashed on matters of detail, requiring businesses and governments alike to arrange processes specific to an increasing array of scenarios.").
[27] *Id.* at 17 (describing how a regulation is uniformly effective across EU).
[28] *See, e.g.*, Regulation 2016/679, *supra* note 1, at 2 (positing individual nations can enforce stricter requirements in some fields, particularly with medical data).
[29] *Id.*

C. Impacts on Compliance Procedures for Financial Institutions

The GDPR affects financial institutions, particularly those employing Fintech platforms and services,[30] in several key areas.[31] The new requirements include obtaining unambiguous affirmative consent, conforming with the "right to be forgotten," notifying authorities of data breaches rapidly, reviewing third-party agreements to ensure outside actors comply with the law, and complying with expanded data portability requirements.[32]

1. Consumer Consent and the "Right to be Forgotten"

The GDPR grants consumers substantial rights to discover how companies utilize their personal data. Prior to collecting or processing most personal data, financial institutions must receive affirmative consent for the collection[33] and for the specific uses of personal data.[34] To meet this consent burden, financial institutions should provide clients with clear statements[35] detailing what personal information the institution collects, and how the data will be processed.[36] Additionally, the GDPR grants clients a right to data erasure, which requires that financial institutions delete client personal data upon request or if clients withdraw consent for data collection.[37] In conjunction with this right, the GDPR grants consumers the right, upon request, to view the personal data an institution has stored.[38] Financial institutions may refuse a data erasure request under the

---

[30] Conheady & Whelan, *supra* note 8.
[31] *See id.* at 1–4.
[32] Regulation 2016/679, *supra* note 1, at 40–41, 43, 45 (outlining rights granted under the GDPR); *see also* Conheady & Whelan, *supra* note 8 (remarking on GDPR requirements most likely to affect financial institutions).
[33] Rob Laplaca, *No Purchase or Personal Data Collection Necessary; GDPR's Impact*, BLOOMBERG BNA (May 2, 2018), https://www.bloomberglaw.com/product/privacy/pds_home/document/XF8SL3J4000000 (discussing GDPR compliance in the context of sweepstakes and contests).
[34] Conheady, *supra* note 8.
[35] *See id.* (detailing methods for clearly presenting information online including directly on the page, through links, pop-ups, and chatbot windows).
[36] *Id.*
[37] *Id.* at 3 (explaining the right to be forgotten).
[38] Regulation 2016/679, *supra* note 1, at 45 (outlining consumers data portability rights).

GDPR when deleting data would create a risk of perpetrating fraud or money laundering by covering a guilty party's tracks.[39] For financial institutions, deciding which requests to refuse for crime prevention purposes presents an ongoing challenge.[40]

2. Providing Appropriate Notification of Personal Data Breaches

The GDPR also imposes data breach reporting standards on financial institutions.[41] All impactful data breaches must be reported to the relevant regulatory agency within seventy-two hours.[42] An implementation challenge for financial institutions involves determining the severity of the breach, and the necessary scope of the notification.[43] In rare instances, the data controller can demonstrate that the breach is minor and that there is almost no risk of infringement of the rights of the affected individuals.[44] Under these circumstances, the controller is not required to report the breach; however, such a determination raises the risk of regulators deeming the breach serious after the fact.[45] On the opposite end of the spectrum, more severe breaches that expose

---

[39] *See* William Long et al., *Guide to GDPR for the Funds Industry*, BRIT. PRIV. EQUITY & VENTURE CAP. ASS'N 21 (2018), https://www.bvca.co.uk/Portals/0/Documents/Media/Guides/BVCA-Guide-to-GDPR-for-the-Funds-Industry.pdf?ver=2018-03-20-175243-727&timestamp=1521737290987 (listing acting in public interest and establishment or exercise of legal claims as exclusions to the right to data erasure).

[40] *See* Eric Geller, *White House Official: 'Cyber Criminals Are Celebrating' New EU Data Rules,* POLITICO (May 16, 2018, 4:55 PM), https://www.politico.eu/article/white-house-official-cyber-criminals-are-celebrating-new-eu-data-rules-gdpr [https://perma.cc/KF6M-QUGW] ("Because the WHOIS database 'will be noncompliant' with the GDPR, Joyce said, it will either have to face the consequences or 'purge the data that makes it useful to find bad actors.'").

[41] *See* Conheady & Whelan, *supra* note 8.

[42] Regulation 2016/679, *supra* note 1, at 16–17 (establishing a 72-hour reporting requirement).

[43] *See* McEvoy, *Know Your GDPR: Self Reporting and Enforcement Considerations for Contentious Regulatory Lawyers,* ALLEN & OVERY LLP (June 26, 2018) http://www.allenovery.com/publications/en-gb/Documents/Allen%20Overy%20Practical%20Law%20June%2018%20GDPR.pdf [https://perma.cc/ZL6K-YWY4].

[44] Long et al., *supra* note 39, at 16–17 (identifying factors to consider when determining the severity and risk associated with a breach).

[45] *See id.* at 17.

consumers to a high risk of infringement of personal rights and freedoms must be reported directly to the affected individuals.[46]

3. Increasing Review of Third-Party Vendor Actions

Financial institutions that share personal data with third-party vendors, either for storage or processing services, must ensure that these third-party vendors remain compliant with the GDPR as well.[47] The GDPR defines the term "data controller" to include the public-facing entity that determines[48] the "purposes and means of the processing of personal data."[49] Financial institutions generally act as data controllers, and in this role, institutions should ensure that the contracts institutions enter into with third-party data processors include all relevant GDPR provisions.[50] These provisions can protect financial institutions from liability for third party violations or allow for indemnification by third parties for fines and damage awards.[51]

4. Data Portability Expansion

The GDPR also contains an expansive data portability provision.[52] At an individual's request, data controllers must provide all the personal data the controller possess about the individual "in a structured, commonly used and machine-readable format."[53] Additionally, upon the individual's request the information must be transmitted to another data controller, directly if possible.[54] This right effectively requires financial institutions to share customer data with third parties approved by the customer.[55]

---

[46] *See id.*
[47] *Id.*
[48] *See* CALDER, *supra* note 3, at 21.
[49] Regulation 2016/679, *supra* note 1, at 33.
[50] *See* Long et al., *supra* note 39, at 17–18.
[51] Conheady & Whelan, *supra* note 8.
[52] Regulation 2016/679, *supra* note 1, at 45 (establishing a right to data portability).
[53] *Id.*
[54] *Id.* ("[T]he data subject shall have the right to have the personal data transmitted directly from one controller to another . . . .").
[55] *See* EUROPEAN BANKING AUTH., REPORT ON INNOVATIVE USES OF CONSUMER DATA BY FINANCIAL INSTITUTIONS 6 (2017), https://eba.europa.eu/documents/10180/1720738/Report+on+Innovative+uses+of+data+2017.pdf

D. Relevance of the GDPR for United States-based Financial Institutions

The GDPR will impact U.S. financial institutions in several ways. First, because of the individual data protection rights mentioned above, the regulation especially impacts institutions operating abroad or soliciting customers in Europe.[56] The GDPR is substantially more comprehensive than current U.S. data privacy regulations,[57] meaning financial institutions operating abroad likely need to update their privacy policies. Second, the GDPR may affect competition in the financial services market within the EU and may disrupt the competitive balance between U.S. and European financial institutions.[58] Third, the GDPR may foreshadow domestic regulation at the state or federal level, benefiting financial institutions that learn from or develop compliance systems for the GDPR in the future.[59]

1. United States Federal Data Privacy Regulation

The FTC serves as the primary federal data privacy regulator within the U.S.[60] Most data privacy laws within the U.S. are fragmented,[61] regulating specific states or industries.[62] The FTC's regulatory authority derives chiefly from enforcing privacy policies that companies issue.[63] Congress granted the FTC regulatory authority to challenge any promissory breach or unfair or deceptive trade

---

[https://perma.cc/CX9F-KSCL] (explaining how regulatory developments like the GDPR will increase data sharing, innovative data usage, and competition).

[56] *See supra* Section III.A–D.

[57] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014).

[58] *See infra* Section D.2.

[59] *See infra* Section D.3.

[60] *See* Solove & Hartzog, *supra* note 57, at 600 (describing how FTC became primary data security regulatory by utilizing their traditional deceptive advertising authority). *But see* Rory Van Loo, *Technology Regulation by Default: Platforms, Privacy, and the CFPB*, 2 GEO. L. TECH. REV. 531, 534 (2018) [hereinafter *Technology Regulation by Default*] (arguing that the CFPB should play a greater role in regulating data security).

[61] *See* Solove & Hartzog, *supra* note 57, at 587 (mentioning that "there are several laws that regulate financial data depending upon the industry").

[62] *See id.* (examining how HIPAA a health insurance regulatory scheme, is superseded by a number of state laws).

[63] *Id.* at 588.

practice.[64] Since most companies have privacy policies in which they offer to protect consumer personal data, the FTC can bring enforcement actions against any company that does not live up to its privacy policy.[65] Due to the tendency for FTC claims to end in settlement, there is very little case law relating to privacy.[66] In comparison, the GDPR provides a comprehensive regulatory scheme, including some of the innovative provisions mentioned above.[67] Financial institutions planning to expand operations into Europe or already operating within Europe will need to update their privacy policies to reflect the more comprehensive standards within the EU.[68] Additionally, data sharing from the EU to U.S. financial institutions may be inhibited if U.S. institutions cannot establish that their data privacy procedures meet the GDPR bar. The Safe Harbor policy, a reciprocal data sharing agreement between the U.S. and EU, is no longer in force due to concerns about lax U.S. data privacy standards.[69] The governments were able to enter a new Privacy Shield framework, but the relative gulf in data privacy regulations makes it likely that further legal challenges will be launched against the framework.[70] As the two governments' policies diverge the traditional transatlantic flow of data may be disrupted in the future.

---

[64] *Id.*

[65] *See id.*

[66] *See id.* at 589 ("[A] large domain of the U.S. privacy regulatory framework primarily consists of a relatively obscure body of doctrines . . . .").

[67] *See supra* Section C.

[68] *Compare* Regulation 2016/679, *supra* note 1, *with* Solove & Hartzog, *supra* note 57, at 606–10.

[69] *See* Mathew J. Schwartz, *EU Court Invalidates U.S.-EU Data Sharing Agreement*, BANK INFO SEC. (Oct. 6, 2015), https://www.bankinfosecurity.com/eu-court-invalidates-safe-harbor-a-8570 [https://perma.cc/G74Q-THTF] ("The Court of Justice of the European Union ruled Oct. 6 that the EU-U.S. data sharing agreement, known as Safe Harbor, is invalid because the United States has failed to ensure that its 'law and practices . . . ensure an adequate level of protection' for Europeans' right to privacy.").

[70] Andrew Karr, *New US-EU Data Sharing Agreement Goes into Effect, but Challenges Await*, GARTNER: TALENT DAILY (July 19, 2016, 10:36 AM), https://www.cebglobal.com/talentdaily/new-us-eu-data-sharing-agreement [https://perma.cc/K55B-YSCL].

2. Data Portability and Financial Competition

One of the intended results of the GDPR is to improve data portability within the EU in order to further innovative processing of personal data that creates economic benefits.[71] The GDPR furthers this goal through the data portability provision, which requires that data controllers share an individual's personal data with other entities upon the individual's request.[72] The GDPR, along with other EU regulatory initiatives,[73] effectively requires that established financial institutions share valuable customer information with other innovative Fintech companies so long as the customer desires the information transfer.[74] European-based Fintech companies, therefore, receive a significant advantage relative to U.S.-based Fintechs, which often struggle to obtain consumer data necessary to develop algorithms[75] since established financial institutions may deny data sharing requests.[76] Data portability helps drive competition in the EU financial services market and positively positions leaner and more adaptable Fintechs within Europe.[77] With the GDPR in place, the likelihood of a Facebook or Google-type Fintech emerging in Europe increases.[78] A successful European Fintech could establish global market share, using first-

---

[71] *See* Regulation 2016/679, *supra* note 1, at 1–3, 11, 25 (elaborating on how GDPR promotes free flow of data between member states and benefits of data sharing).
[72] *Id.* at 45.
[73] *See, e.g.*, EUROPEAN BANKING AUTH., *supra* note 60, at 6–7.
[74] *See Technology Regulation by Default*, *supra* note 60, at 535 ("European authorities have required banks to give third parties far-reaching access to data upon consumer authorization.").
[75] *See id.* (examining how Fintech companies like Mint and Credit Karma rely on customer financial data possessed by banks to advise customers and how banks have obstructed third-party access to customer data threatening Fintechs effectiveness).
[76] Rory Van Loo, *Rise of the Digital Regulator*, 66 DUKE L.J. 1267, 1286 (2017) (describing how major financial institutions attempt to block Fintechs access to data despite customer protests regarding efforts to block third-party access).
[77] *See The Case of Fintech*, *supra* note 10, at 253 ("Foreign financial firms may gain an edge by being subject to greater competition in their home markets, thereby being forced to innovate more and operate leanly).
[78] *Id.* at 248.

mover advantages to outmaneuver other startups and compete with established U.S. financial institutions.[79]

Additionally, through the Dodd-Frank Act, Congress tasked the Consumer Financial Protection Bureau (CFPB) with studying and regulating data portability within the United States.[80] The CFPB, while largely inactive under the current executive leadership,[81] announced data portability principles in the fall of 2017.[82] The CFPB may eventually adopt data portability rules similar to those outlined in the GDPR.[83] The GDPR could, therefore, provide U.S.-based financial institutions with a test case of how data portability rules may impact them.

3. California's Data Privacy Law

Individual states that implement policies reflecting the GDPR can help prepare U.S.-based financial institutions for future privacy laws. On June 28, 2018, California enacted the California Consumer Privacy Act of 2018 (CCPA) which becomes effective January 1, 2020.[84] The CCPA, while distinct from the GDPR, adopts several of the critical concepts established by the GDPR.[85] These parallel concepts include the "right to be forgotten" and the treatment of

---

[79] *See id.* at 253.

[80] *See Technology Regulation by Default*, *supra* note 60, at 534 (remarking that "Congress has mandated that the CFPB study how best to regulate the sharing of information between financial institutions and third parties . . . .").

[81] *See* Ken Sweet, *Under Trump and Mulvaney, CFPB Has Filed No Enforcement Actions since November,* USA TODAY (Apr. 10, 2018, 10:52 AM), https://www.usatoday.com/story/money/economy/2018/04/10/under-trump-mulvaney-cfpb-has-filed-no-enforcement-actions/502451002 [https://perma.cc/N3R8-FJ5B].

[82] *See Technology Regulation by Default*, *supra* note 60, at 535 (citing CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf [https://perma.cc/8N4B-SKJM] (explaining the necessity for consumer protection and data portability principles)).

[83] CONSUMER FIN. PROT. BUREAU, *supra* note 82, at 2–3.

[84] Hirsh & Hadgis, *supra* note 13.

[85] *See id.* (comparing GDPR and CCPA structures).

institutions as "data controllers."[86] Due to the sheer size of California's population, the CCPA will affect almost all major U.S.-based financial institutions,[87] and may inspire other states to pass similar data privacy legislation. Financial institutions operating within the EU and California can benefit from the policies and experiences they have under the GDPR to more seamlessly comply with the CCPA.[88] Both regulations require financial institutions to conduct data mapping and privacy assessments in order to establish the infrastructure necessary to comply with the regulations, and prior work will benefit institutions as they prepare for the CCPA.[89] The experience compliance institutions develop while navigating the GDPR can also prove valuable in preparing for the CCPA and other future data privacy enactments.

E. Challenges for Financial Institutions Navigating the GDPR

For major financial institutions, the possible fines are sufficient motivation to avoid violations of the law.[90] Fines range from $20 million upwards to four percent of all global revenues for the past year,[91] a figure that could easily exceed a billion dollars for many major financial institutions.[92] Additionally, companies found in violation will need to account for costs of investigation, response activities, and corrective action.[93] These costs—including lost revenues and

---

[86] *Id.* (observing that the CCPA's "technical feasibility" and "right to be forgotten" standards appear to be pulled directly from the GDPR).
[87] *See id.*
[88] *See id.*
[89] *Id.*
[90] *See General Data Protection Regulation: Are You Prepared?*, BRICKENDON CONSULTING LTD. 2 (2017), https://www.brickendon.com/wp-content/uploads/2017/09/Brickendon-Consulting-Insight-GDPR-are-you-prepared-digital-UK.pdf [https://perma.cc/34DC-LX8Y].
[91] Regulation 2016/679, *supra* note 1, at 82, 83 (enumerating maximum penalties for violations).
[92] *See* Halah Touryalai & Kristin Stoller, *Global 2000: The World's Largest Public Companies 2018,* FORBES (June 6, 2018, 6:00 PM), https://www.forbes.com/global2000/#8a4fa77335d8 [https://perma.cc/JC6B-NL3G].
[93] Louis Alberto Montezuma & Qian Li Loke, *Privacy Compliance Matters to a Company's Valuation*, INT'L ASS'N OF PRIVACY PROF'LS (Aug. 28, 2018), https://iapp.org/news/a/privacy-compliance-matters-to-a-companys-valuation [https://perma.cc/A36J-K5WU].

potential suspension of online business—may impact operating results of financial entities and devalue rising Fintech companies.[94]

However, institutions can mitigate costs and fines by clearly documenting their data protection processes and commitment to data security.[95] The GDPR enforcement provision considers institutional negligence, mitigation efforts, and cooperation in determining the extent of any fine imposed.[96] Affirmative compliance actions and documented safety procedures will help financial institutions display their commitment to data security and limit the risk of consequences under the GDPR.[97] These actions, while costly upfront, can reduce long-term costs and pay dividends for future operations.

Financial institutions also face the challenge of competing regulatory institutions. Financial institutions often face audits and may otherwise need to maintain client personal data for extended periods as part of their operations.[98] The GDPR encourages financial institutions to delete personal data as quickly as possible, which creates opposing dynamics for financial institutions. For example, in the United Kingdom, the Information Commissioner's Office (ICO), the entity primarily in charge of enforcing the GDPR, and the Financial Conduct Authority (FCA) have some competing standards.[99] While the ICO and FCA have collaborated and announced that their regulations do not conflict,[100] in some instances complying with the GDPR may encourage deleting personal data, while complying with financial regulations may motivate companies to save personal data.[101] Complying with other regulatory requirements is one of the GDPR's exceptions to the "right to be forgotten" and is a valid reason to maintain personal

---

[94] *Id.*
[95] *See* McEvoy, *supra* note 43.
[96] Regulation 2016/679, *supra* note 1, at 82 (outlining method for determining fines).
[97] *Id.*
[98] UK Fin., Frequently Asked Questions on the General Data Protection Regulation (GDPR) 3, https://www.ukfinance.org.uk/wp-content/uploads/2018/05/GDPR-FAQ-FINALv2.pdf [https://perma.cc/G23D-54KJ].
[99] McEvoy, *supra* note 43, at 2.
[100] Joint Update, Fin. Conduct Auth. & Info. Comm'rs Office, FCA and ICO Publish Joint Update on GDPR (Feb. 13, 2018), https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr [https://perma.cc/VW6G-RSXQ] ("We believe the GDPR does not impose requirements which are incompatible with the rules in the FCA handbook.").
[101] McEvoy, *supra* note 43, at 1.

data.[102] Clear documentation of the decision-making process and elaborated reasoning of why data was maintained or deleted will aid financial institutions in dealing with either the ICO or FCA after the fact.[103]

F. Conclusion

The GDPR unifies data privacy regulation throughout the EU by providing multinational financial institutions an opportunity to add efficiency through standardization.[104] As noted above, over the twenty-year period following the issuance of the DPD, no EU member nations issued data privacy laws that were consistent with or complementary to all other member nations.[105] The GDPR upended this reality, creating a single regulatory environment under which an institution can maintain a unified compliance policy for all its EU based operations.[106] The GDPR revolutionizes the way financial institutions operating within the EU must monitor and utilize their customers' personal data. While the regulation adds additional regulatory requirements for financial institutions, it also simplifies data privacy regulation by creating a unified, enforceable legal system. New consumer consent rights and increased scrutiny of financial institution decision making presents a challenge for financial institutions, but one that institutions can adapt to by implementing proper compliance processes. Additionally, the GDPR is likely only the first of many stringent personal data protections to come around the world. As technology continues to advance, more governments will follow the EU's lead in implementing strong consumer personal data protection. Financial institutions with sophisticated data privacy compliance infrastructure can benefit when adapting to new laws. The GDPR presents an

---

[102] *See* Long, *supra* note 39, at 21.
[103] *Id.*
[104] *See* Regulation 2016/679, *supra* note 1, at 2 (stating legislative goal to "remove the obstacles to flows of personal data within the Union" contrasts with the previously fragmented data protection framework, where inconsistent levels of protection "may prevent the free flow of personal data throughout the Union … therefore constitute[ing] an obstacle to the pursuit of economic activities at the level of the Union").
[105] *See* CALDER, *supra* note 3, at 16.
[106] Regulation 2016/679, *supra* note 1, at 2, 3 (covering goals of GDPR including free flow of data across borders and proper protection of consumers in digital world).

ongoing challenge for financial institutions but is by no means insurmountable.

Tyler Stites[107]

[107] Student, Boston University School of Law (J.D. 2020).