UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 23 | Issue 1 Article 13

3-1-2019

GDPR: Navigating Compliance as a United States Bank

Lindsay A. Seventko

GDPR: NAVIGATING COMPLIANCE AS A UNITED STATES BANK

I. INTRODUCTION

Data is the "gold of the 21st century,"[1] and as such it is only fitting that big banks are on the forefront of capitalizing on customer data, even down to analyzing how individuals hold their phones and scroll through Instagram.[2] The European Union's (EU's) new General Data Protection Regulation ("GDPR") that took effect on May 25, 2018[3] has been criticized as "business killing" in the popular media[4] and may be especially problematic for large banks seeking to capitalize on their state of the art customer tracking systems.[5]

GDPR was designed to prevent issues like the Facebook Cambridge Analytica data scandal and to provide a method of punishing companies with relaxed data security protocols by levying significant fines.[6] By strengthening data protection rules, the European Commission sought

---

1. Shannon Tellis, *Data Is the 21st Century's Oil, Says Siemens CEO Joe Kaeser*, THE ECON. TIMES (May 24, 2018), https://economictimes.indiatimes.com/magazines/panache/data-is-the-21st-centurys-oil-says-siemens-ceo-joe-kaeser/articleshow/64298125.cms ("Data is the oil, some say the gold, of the 21st century—the raw material that our economies, societies and democracies are increasingly being built on.").

2. *See* Stacy Cowley, *Banks and Retailers Are Tracking How You Type, Swipe and Tap,* N.Y. TIMES (Aug. 13, 2018), https://www.nytimes.com/2018/08/13/business/behavioral-biometrics-banks-security.html (discussing that banks are using this information to fight fraud because "[t]he way you press, scroll and type on a phone screen or keyboard can be as unique as your fingerprints or facial features").

3. *See* EUR. COMMISSION, A NEW ERA FOR DATA PROTECTION IN THE EU: WHAT CHANGES AFTER MAY 2018, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf [hereinafter A NEW ERA] (providing high-level information on what changes in data protection law after GDPR takes effect).

4. *See* Ivana Kottasová, *These Companies Are Getting Killed by GDPR*, CNN MONEY (May 11, 2018), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html (discussing that small businesses in particular will struggle to stay in business with the costs of complying with GDPR).

5. *See* Mark Nicholls, '*Boiling the Ocean': GDPR Data Demands Overwhelm Banks*, RISK.NET (July 6, 2017), https://www.risk.net/risk-management/5299086/boiling-the-ocean-gdpr-data-demands-overwhelm-banks ("'The biggest challenge around GDPR is that the legislation is so voluminous. We did a gap analysis and found we're not complying with any of it,' says one London-based operational risk specialist at a non-European bank.").

6. *See* A NEW ERA, *supra* note 3 ("The Facebook/Cambridge Analytica revelations show the EU has made the right choice to propose and carry out an ambitious data protection reform through the General Data Protection Regulation (GDPR).").

to even the playing field between businesses and to increase individuals' autonomy over their data.[7] In furtherance of those goals, the Commission focused on regulating five main areas: (1) requiring companies to write privacy policies "in a clear, straightforward language"; (2) requiring companies to obtain "an affirmative consent" from a user before the company can use the user's data; (3) encouraging companies to increase transparency in how and why customer data is transferred, processed, and used in automated decision making; (4) giving data subjects stronger rights over their data; and (5) giving the European Data Protection Board strong enforcement authorities.[8]

These areas of expanded regulation present significant challenges for the banking industry because banks typically acquire, store, and process a large amount of data as a central part of their operations.[9] Large international banks have a compliance advantage over smaller, domestic-only banks because they are accustomed to complying with the previous EU privacy directive that addressed similar principles.[10] However, GDPR "looks to be the furthest reaching and most complex data-stewardship regulatory scheme the world has ever seen,"[11] leaving even large banks

7. *See* EUR. COMM'N, 2018 REFORM OF EU DATA PROTECTION RULES, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#abouttheregulationanddataprotection (last visited Jan. 10, 2019) [hereinafter 2018 REFORM] (proposing that GDPR will "mean people have more control over their personal data and businesses benefit from a level playing field.").

8. *EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation),* O.J. 2016 L 119/1 [hereinafter GDPR]*; see also* A NEW ERA, *supra* note 3 (providing an overview of the Commission's goals and primary areas of regulatory focus); *see also* EDPB, *About EDPB,* https://edpb.europa.eu/about-edpb/about-edpb_en (last visited Jan. 13, 2019) (discussing that the EDPB is "an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.").

9. *See* Gina Conheady & John Whelan, *EU GDPR: 10 Things Every Fintech Business Should Know,* BIG LAW BUS. (Aug. 10, 2018), https://biglawbusiness.com/eu-gdpr-10-things-every-fintech-business-should-know/ ("The ability and capability to freely process personal data is key to almost every fintech business.").

10. *See* Penny Crosman, *Large U.S. Banks Scramble to Meet EU Data Privacy Rules*, AM. BANKER, Apr. 17, 2018 (including a quote from an IBM GDPR specialist that says banks "shouldn't be starting from a blank slate . . . they are hopefully already meeting some of the privacy and security needs.").

11. Joe Stanganelli, *My Cybersecurity Predictions for 2018, Part 2: GDPR Hype is Hype*, SECURITYNOW (Dec. 1, 2017), https://www.securitynow.com/author.asp?section_id=613&doc_id=739226.

scrambling to interpret the law's ambiguities and to determine how to comply.[12]

The previous EU privacy directive, Directive 95/46/EC, was applauded as a landmark in privacy and human rights law upon its adoption in 1995 and has been widely used by the European Court of Human Rights to further consumer protections.[13] It laid the groundwork for GDPR by broadly defining personal data and mandating that personal data cannot be processed unless adequate measures surrounding transparency, explicit legitimate purposes, and proportionality are undertaken.[14] Since its implementation, however, the case law interpreting Directive 95/46/EC varied across Member States, resulting in inconsistent treatment of similar actions across the European Union.[15]

GDPR was developed primarily in response to frustrations about those inconsistent applications of Directive 95/46/EC across Europe, and to establish a method of addressing these legal uncertainties.[16] While GDPR is more comprehensive and further reaching than the Directive 95/46/EC, and by its nature is more binding because it is a regulation, it is unclear how GDPR will avoid the same varied interpretation pitfalls seen by Directive 95/46/EC.[17] When GDPR took effect on May 25, 2018, it established the European Data Protection Board ("EDPB"), which is the main regulatory body that issues guidance and recommendations with regard to the consistent application of GDPR across Member States; however, it is ultimately up to each Member State to develop their own interpretations and to determine how the regulation will apply in their country.[18] Navigating multiple enforcement authorities could prove problematic in the case of international processing, such as when an

12. *See* Nicholls, *supra* note 5 (quoting an operational risk specialist at a non-European bank who says, "to comply with everything is effectively like trying to boil the ocean—so we decided that while we needed to go hard on certain things, we could go a bit lighter on others.").

13. *See* Rachel de Vries, *The European Legal Context: EU Data Protection,* LEGAL INFO. INST. (Aug. 2017), https://www.law.cornell.edu/wex/inbox/european_legal_context_privacy_directives (discussing the European Parliament's approach to data protection as a human right).

14. *Id.*

15. *Id*.

16. *Id*.

17. *Id*.

18. *See* Jenna Kersten, *Who's Enforcing GDPR*?, KIRKPATRICKPRICE (July 19, 2018) https://kirkpatrickprice.com/blog/whos-enforcing-gdpr/ (noting that the EDPB replaced the Article 29 Working Party without significant changes to its structure or authority, making it unlikely that the EDPB will be particularly more effective at maintaining consistent interpretations than its predecessor).

Austrian customer's data is processed by a German-based bank and stored on servers in Switzerland.[19] In such a scenario, the supervisory authorities from all three Member States would need to collaborate in an enforcement action.[20] Due to the data processing actually taking place by a German bank, the German supervisory authority would take the lead among the three member states.[21]

Questions of consistent implementations aside, GDPR strengthens the consumer privacy rights first outlined in the Directive 95/46/EC both substantively and by virtue of its jurisdictional reach. GDPR applies even to those companies based outside of the E.U. that are monitoring the behavior of consumers in the E.U. or even simply marketing goods or services to individuals in the E.U.[22] Substantively, it greatly strengthens the principles of privacy by design and default, emphasizing the premise that entities should orient both their user experience and back-end processes so that individuals have control over their data.[23]

Implicit in GDPR's reach is the nearly forgone conclusion that large, international banks will certainly need to comply with GDPR, regardless of where they are headquartered or primarily conducting business.[24] The more difficult question is whether smaller, regional U.S. banks will need to comply with GDPR. As many as 50% of businesses may be mistakenly out of compliance with GDPR.[25] With a penalty of four percent of revenue at stake,[26] smaller domestic banks should carefully examine whether they fall within the scope of with GDPR, and if so, how they can effectively ensure compliance.

This Note proceeds in five parts. Part II addresses interpretations to the entry-level question of when GDPR applies by examining

---

19. *See, e.g., id.* (discussing when multiple regulatory bodies may be involved).

20. *See id*. (discussing the interplay of various regulatory actors).

21. *See id*. ("If there is cross-border processing, the supervisory authority of the main establishment acts as a lead supervisory authority.").

22. *See* Monica Meinert, *GDPR: These Four Letters Could Spell a Compliance Headache for Smaller Banks,* ABA BANKING J. (February 23, 2018), https://bankingjournal.aba.com/2018/02/gdpr-these-four-letters-could-spell-a-compliance-headache-for-smaller-banks/ ("[How many] of their customers are in the EU and if they are regularly doing business with and/or marketing to them . . . [is] going to be an indicator as to whether or not this law applies to them . . . .").

23. *See id*.

24. *See id.* ("[G]lobal banks already know that [GDPR] applies to them . . . .").

25. *See* Caroline Spiezio, *Over Half of Companies Are Far From GDPR Compliance, Report Finds*, LAW.COM (Oct. 19, 2018), https://www.law.com/corpcounsel/2018/10/19/over-half-of-companies-are-far-from-gdpr-compliance-report-finds/ ("[M]ore than half of respondents, 56 percent, said they are far from compliant or will never fully comply.").

26. See *infra* part IV (discussing penalties for noncompliance).

interpretations of who is considered a covered data subject, what constitutes personally identifiable information, and who identifiable natural people are.[27] Part III examines the main overarching principles of the GDPR and offers suggestions for how banks can integrate them via the technique of privacy by design.[28] Part IV discusses penalties for noncompliance and potential causes of action given to data subjects.[29] Part V summarizes the recommendations given throughout this Note.[30]

II. WHEN DOES GDPR APPLY?

The introductory question is, of course, whether GDPR even applies to a domestic bank.[31] Unfortunately, the answer to that question is unclear, as three different, equally plausible interpretations of the ambiguous text have emerged.[32] This section explores possible interpretations of GDPR's territorial scope.

A. Establishments in the European Union

GDPR "applies to the processing of personal data in the context of activities of an establishment of a controller or a processor in the [European] Union, regardless of whether the processing takes place in the Union or not."[33] The first step in determining whether GDPR applies, therefore, is to determine if the bank has an establishment in the Union.[34]

Banks that have European offices are considered established in the Union.[35] Beyond that, banks that market or sell services to Europeans

27. *See infra* Part II.

28. *See infra* Part III.

29. *See infra* Part IV.

30. *See infra* Part V.

31. *See* Jingnan Huo, *EU's New Data Privacy Law Creates Headaches for U.S. Banks*, AM. BANKER 1, 3, Sept. 20, 2017, https://www.americanbanker.com/news/eus-new-data-privacy-law-creates-headaches-for-us-banks ("U.S. banks—especially small and midsize banks—need to go find out because the [GDPR] could affect them, unlike the EU privacy regulations before it.").

32. *See* Joe Stanganelli, *GDPR Territorial Scope: Location, Location, Location?*, SECURITYNOW (Feb. 16, 2018), https://www.securitynow.com/author.asp?section_id=613&doc_id=740638 ("There are a few perfectly valid interpretations out there . . . GDPR is so massive and . . . so broadly-worded, that no one can really be sure how the DPAs will interpret the minutiae of it until they start applying it.").

33. *GDPR*, *supra* note 8, at art. 3(1).

34. *See id*. ("Obviously, GDPR applies to (1) data controllers and data processors sufficiently established within the EU . . . . ").

35. *See* Crosman, *supra* note 10 ("Banks that have European offices have to [comply].").

are also considered to have an establishment in the Union.[36] Whether a bank is marketing to a European comes down to the bank's demonstrated intention.[37] While simply making a website available to Europeans would not be enough to establish intention,[38] the use of a European language or currency with the sole purpose to facilitate a transaction would likely create an establishment in the Union and trigger compliance.[39] Other factors that indicate an intent to market to Europeans include mentioning a telephone number with a European code, using a domain name ending in ".eu," or offering a conversion of prices into EU currency.[40] The Court Justice of the European Union has held that "patent" evidence of intention to market to Europeans involves purchasing advertisements targeted to a European geographic area.[41]

B. EU Data Subjects

Even if a bank does not have an establishment in the Union, a bank will likely need to comply with GDPR under Article 3 § 2:

> This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union.[42]

---

36. *See* Crosman, *supra* note 10 (suggesting that banks which market to Europeans by translating a website into a European language have to comply with GDPR).

37. *See* Conheady & Whelan, *supra* note 9 (asking whether "it is apparent that an offer to an EU-based data subject was envisaged.").

38. *GDPR, supra* note 8, at art. 3(1).

39. *See* Conheady & Whelan, *supra* note 9 (discussing the line between mere availability and sufficient intention to offer goods or services to individuals in the European Union).

40. *See* Kevin Kish, *What Does Territorial Scope Mean Under GDPR?*, INT'L ASS'N OF PRIVACY PROFS. (Jan. 23, 2018), https://iapp.org/news/a/what-does-territorial-scope-mean-under-the-gdpr/ (discussing the factors that contribute to whether an organization is likely to be determined an establishment in the European Union).

41. *See id*. ("'Patent' evidence, such as the payment of money to a search engine to facilitate access by those within a member state or where targeted member states are designated by name . . . . ").

42. *GDPR*, *supra* note 8, at art. 3(2).

Banks are taking one of three approaches to who a data subject "in the Union" is, based on the bank's risk profile and likelihood of being targeted for an enforcement action.[43] Essentially, a data subject in the Union could be a citizen of the EU, a resident of the EU, or merely a person temporarily in the EU.[44] There is arguably no "correct" approach yet, as each approach is plausible, and the European Commission has not yet brought an enforcement action which fully answers this question.[45] The interpretation a bank chooses is largely a business decision and reflects the growing trend of cybersecurity-related decisions being made at the C-suite level, largely because of the significant penalties at stake.[46] Smaller, U.S. community banks may not bother to comply with GDPR, even if they technically are within its purview, because enforcement actions are likely to initially target big institutions that control more consumer data.[47] Conversely, large financial institutions may want to choose a conservative reading of the text in order to hedge their bets against a potentially astronomically costly enforcement action.[48] Considering those large institutions may be subject to a fine of four percent of worldwide gross revenue per instance of violation, chief financial officers

43. *See* Crosman, *supra* note 10 ("It's not crystal clear which U.S. banks must comply.").

44. See *infra* Section II(B)(1–3).

45. At the time of publication, no enforcement action clearly answering this question on territorial reach has been undertaken by a supervisory authority. *See* EUROPEAN DATA PROTECTION BOARD, *National News,* (2018) https://edpb.europa.eu/news/national-news/2018_en (posting official press releases from supervisory authorities about all fines imposed or actions taken to date).

46. *See* HERJAVEC GROUP, CYBERSECURITY CONVERSATIONS FOR THE C-SUITE IN 2018, (2018), https://www.herjavecgroup.com/wp-content/uploads/2018/07/Cyber-Conversations-for-the-C-Suite-2018_HG.pdf (suggesting that GDPR is the most noteworthy regulation that should be talked about at the executive level); *see also* Rao Papolu, *In the Wake of GDPR, It Can't be Business As Usual with Consumer Data Privacy,* FORBES (Sept. 18, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/09/18/in-the-wake-of-gdpr-it-cant-be-business-as-usual-with-consumer-data-privacy/ (naming 2017 "the year of the data breach" and GDPR the "global regulatory wake up call").

47. *See* Crosman, *supra* note 10 ("I don't know that if I had one European customer I would go through the effort of complying with GDPR . . . [b]ut technically, you would be subject to GDPR."); *see also* Adam Satariano, *Google is Fined $57 Million Under Europe's Data Privacy Law*, N. Y. TIMES (Jan. 21, 2019) https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html ("[This enforcement action] shows that regulators are following through on a pledge to use the rules to push back against internet companies whose businesses depend on collecting data. Facebook is also a subject of several investigations by the data protection authorities in Europe.").

48. *See* Abi Miller, *GDPR: How Is It Affecting Banks?*, FIN. DIRECTOR (June 21, 2018), https://www.financialdirector.co.uk/2018/06/21/gdpr-how-is-it-affecting-banks/ (pointing out that previously the ICO could impose a €500,000 fine, but under GDPR they could impose €20million or 4% of global revenue, whichever is larger, and calling this a wake up call for banks).

unsurprisingly recommend sparing no expense on GDPR compliance after running a cost-benefit analysis.[49] This section discusses the three main emerging interpretations of Article 3 § 2.

1. Citizen of the EU

Some financial institutions are interpreting "data subjects in the Union" to mean a citizen of the EU, regardless of whether that citizen is residing in a European country or elsewhere around the world.[50] This approach makes the most sense for small, local banks because the costs of a comprehensive compliance scheme may be prohibitively high, and EU regulators are likely to target big names first before moving down to smaller institutions.[51] However, citizenship can be hard to determine from the limited data a bank is likely to have about the subject, and can create the problem of needing to ask for additional information.[52] For U.S.-based banks that process E.U. citizens' data, this interpretation would require putting in extra steps to determine whether their current and potential customers are E.U. citizens.[53] While this may be a costly endeavor to undertake for some banks, it is a step that some U.S. banks are already taking.[54] On a risk-reward basis, smaller banks are unlikely to be targeted by the Commission in the first few years of enforcement,

---

49. *See* Nina Trentmann, *Companies Worry that Spending on GDPR May Not be Over,* WALL ST. J. (May 25, 2018), https://www.wsj.com/articles/companies-worry-that-spending-on-gdpr-may-not-be-over-1527236586 (quoting Harm Ohlmeyer, CFO of Adidas saying "you cannot spend enough to protect yourself," and discussing that "around 60% of companies surveyed by PricewaterhouseCoopers LLP said they would spend more than $1 million in preparing for GDPR, while 12% reported allocating more than $10 million").

50. *Does GDPR Apply to EU Citizens Living in the US?*, HIPAA JOURNAL (May 11, 2018), https://www.hipaajournal.com/does-gdpr-apply-to-eu-citizens-living-in-the-us/ (suggesting that "citizen" is probably not the most accurate interpretation of the regulation, but that it may make for more straightforward compliance).

51. Laurens Cerulus & Mark Scott, *Who Stands to Lose Most from Europe's New Privacy Rules,* POLITICO (May 23, 2018), https://www.politico.eu/article/the-gdpr-hit-list-who-stands-to-lose-from-europes-new-privacy-rules-facebook-google-data-protection/ (highlighting that Google, Apple, Facebook, Amazon and Microsoft will likely be targeted first, but that banks are likely targets as well because they "have always held large sets of personal data").

52. *See* Robert Madge, *Five Loopholes in the GDPR*, MEDIUM (Aug. 27, 2017) https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b (discussing that if a controller cannot identify a subject, the subject can provide more information to aid the identification).

53. *See* Crosman, *supra* note 10 (briefly discussing the need to determine the extent to which the company's customer base includes EU citizens).

54. Agatha Pacheco, *Bank of America Will Begin Asking About Citizenship Status*, THE SEATTLE GLOBALIST (Apr. 13, 2018), https://www.seattleglobalist.com/2018/04/13/bank-asks-about-citizenship/73372.

and the costs involved in reaching compliance with a stricter GDPR reading—such as one that protects E.U. residents or U.S. citizens temporarily traveling in the E.U.—could reach into the tens of millions.[55] As one Information Security Director stated, "realistically, if you have one European customer, nobody is going to come after you for GDPR violations, you're so far down in the priority of regulatory review . . . But technically, you would be subject to GDPR."[56]

2. Resident of the EU

Other banks have taken the position that "GDPR is not concerned with citizenship . . . [and] the term EU resident is more useful."[57] This approach makes more sense in light of ease of compliance because it is fairly easy to determine whether data subjects have an E.U. address—whether physical or IP—and therefore fairly easy to make a quick determination about whether the GDPR protocols and protections apply to this subject.[58] In a practical sense, if banks do not have a way of determining if GDPR conveys rights on the data subject, they will either need to expend exorbitant amounts of money treating U.S. citizens as E.U. citizens, or they will risk being out of compliance, whether discovered by a regulator or upon a request from a data subject. Therefore, this interpretation is probably the most widely implemented and is a sensible, middle-of-the-road interpretation for banks to follow until the first enforcement action clears up the ambiguity.

3. Person in the EU

The most conservative interpretation of "data subjects in the Union," and perhaps the one with the most textual support, is that GDPR protections are triggered by a consumer's physical presence in the E.U.,

---

55. Trentmann, *supra* note 49.

56. Crosman, *supra* note 10 (quoting Jeff Sanchez, the managing director of information security and privacy at Protiviti, and discussing his opinion that "for smaller community and regional banks, it's more dependent on their analysis of what their customer base looks like and what their exposure to European data subjects is.").

57. *See Does GDPR Apply to EU Citizens Living in the US?*, HIPAA JOURNAL (May 11, 2018), https://www.hipaajournal.com/does-gdpr-apply-to-eu-citizens-living-in-the-us/ (suggesting that GDPR applying to EU residents is probably the most practical interpretation).

58. *See* Cale Guthrie Weissman, *What Is an IP Address and What Can It Reveal About You?*, BUS. INSIDER (May 19, 2015), https://www.businessinsider.com/ip-address-what-they-can-reveal-about-you-2015-5 (saying an IP address reveals city-level location data).

regardless of citizenship or residency.[59] Recital 14 of the GDPR states that "[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data."[60] Banks have interpreted this to mean that "what matters is where a person is when they're communicating with the bank."[61] Therefore, banks processing the data of customers who are located in the EU at the time of the processing will need to comply with GDPR.[62] For example, GDPR protections would arise from "banks monitoring their customers' transaction activity while they are traveling within the EU."[63]

In light of the likelihood that large, international banks will be targeted in an enforcement action, they should consider adopting this conservative interpretation.[64] To do so, they would need to first perform a full review of existing customers to determine which are EU citizens or residents.[65] Beyond that, they would need to put in place a process for customers who are traveling or temporarily living in the EU, so that they are able to comply with GDPR for those short periods of time.[66] In a practical sense, the process of GDPR compliance is likely not something that a bank can easily switch on and off.[67] Instead of creating a complex compliance regime designed for temporary compliance, banks may be

59. Moyn Uddin, *GDPR – The Data Subject, Citizen or Resident?*, CYBER COUNS. (Jan. 29, 2017), https://cybercounsel.co.uk/data-subjects/ ("A data subject under GDPR is anyone within the borders of the EU at the time of processing of their personal data.").

60. *GDPR*, *supra* note 8, at Recital 24.

61. Crosman, *supra* note 10 ("[A]n Irish citizen living in a New York condo with a New York bank mortgage, for instance, is not subject to GDPR.").

62. *See Does GDPR Apply to EU Citizens Living in the US?*, HIPAA JOURNAL (May 11, 2018), https://www.hipaajournal.com/does-gdpr-apply-to-eu-citizens-living-in-the-us/ ("Anyone located in an EU country is protected by GDPR.").

63. *GDPR Non-Compliant APAC Firms Liable for Class Actions*, 20 CLASS ACTION REP., July 26, 2018.

64. *See* Cerulus, *supra* note 51 (suggesting that banks will likely be targeted for GDPR enforcement actions).

65. *See* FENERGO, GDPR: GAME CHANGER FOR MANAGING DATA & REGULATORY COMPLIANCE, (Sept. 2017), https://www.fenergo.com/resources/whitepapers/gdpr-managing-data-protection.html [hereinafter Fenergo] ("[T]he first logical step in complying with GDPR is to undertake an audit to assess how much and which data processing activities are subject to GDPR obligations.").

66. *See id.* (discussing this approach in the context of implementing a privacy by default strategy).

67. *See GDPR Deep Dive—How to Implement the 'Right to be Forgotten'*, BANKINGHUB (Nov. 15, 2017), https://www.bankinghub.eu/banking/finance-risk/gdpr-deep-dive-implement-right-forgotten (discussing that GDPR compliance will likely be a challenge for banks, which often have large, complex data systems).

better off being over-inclusive with their compliance regime.[68] With GDPR-esque regulations slated to take effect in the U.S. in the next few years, taking a conservative stance on GDPR interpretation now would give banks a leg-up in navigating any U.S. counterparts, such as the California Consumer Privacy Act and the federal Social Media Privacy Protection and Consumer Rights Act.[69]

C. What is Personally Identifiable Information?

The EU's concept of personally identifiable information ("PII") is counterintuitive to many American lawyers and compliance personnel.[70] PII in the United States is typically defined as the type of data that are commonly used for authenticating an individual, such as a Social Security number, driver's license number, or financial accounts.[71] However, GDPR defines personal data as "any information . . . concerning an identified or identifiable natural person."[72]

1. What is an Identified or Identifiable Natural Person?

Information that concerns an identified or identifiable person for GDPR purposes takes on a very literal meaning—it could be as simple as a name, number, IP address, or cookie identifier, which is a unique packet of data that a website receives from the user's computer and sends back to keep track of an online visitor's traffic and activity.[73] Beyond these

68. *See* Ashwani Verma, *GDPR is now law. Is your business fully compliant?,* SILICON VALLEY BUS. J. (June 27, 2018) https://www.bizjournals.com/sanjose/news/2018/06/27/gdpr-is-now-law-is-your-business-fully-compliant.html (advocating that businesses "err on the side of caution" when deciding whether or not they need to comply with GDPR).

69. *See* Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, HARV. BUS. REV. (July 11, 2018), https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law (discussing the new rights that will be afforded California residents over their data); *see also* Social Media Privacy Protection and Consumer Rights Act of 2018, S. 2728, 115th Cong. (2018), https://www.congress.gov/bill/115th-congress/senate-bill/2728.

70. *See* Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security: Myths and Fallacies of "Personally Identifiable Information,"* 53 COMM. OF THE ACM 24, 24 (2010), https://www.cs.cornell.edu/~shmat/shmat_cacm10.pdf (discussing the differences in the concept of PII between European and U.S. privacy regulations).

71. *See id.* (discussing the differences in the concept of PII between European and U.S. privacy regulations).

72. *GDPR*, *supra* note 8, at Recital 26.

73. *See What Is Personal Data?*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-

obvious identifiers, it could also be an internal-only reference number to a customer's complaint or question.[74] Essentially, it means any piece of data that can be tied to a specific person, no matter how seemingly trivial.[75] Even pseudonymous data is included.[76]

Even if a bank cannot directly identify an individual from a piece of data, the individual may still be identifiable and therefore also fall under GDPR protections.[77] A person is identifiable under GDPR if they can still be identified indirectly through the accumulation of non-individually identifying data.[78] To determine if a data subject is identifiable, banks should take into account both the data being processed and the means that would be required to identify that person.[79] While an individual may be identifiable with enough time, money, technology, and effort, the determination is a practical one.[80] Taking into account all the factors, how likely is it that that this person will be identifiable?[81]

What banks may be dismayed to learn is that identifiable information includes data that has undergone pseudonymisation, which is the process of "replacing personally identifiable material with artificial identifiers."[82] Even though pseudonymisation will not eliminate GDPR compliance obligations, banks should still utilize it as an extra layer of

---

personal-data/ (last visited Jan. 15, 2019) (defining "data subject" as an identified or identifiable natural person and providing examples identifying information).

74. *See* Rhys Dipshan, *How Much Will the GDPR Change Consumer Technology?*, THE RECORDER (CAL.) (Dec. 27, 2017) (discussing the true breath of identifying information); *see also* Symantec, *What Are Cookies?*, NORTON, https://us.norton.com/internetsecurity-privacy-what-are-cookies.html (last visited Jan. 16, 2019) (discussing how browser cookies work and the information they convey).

75. *See* Luke Irwin, *The GDPR: What Exactly Is Personal Data*?, IT GOVERNANCE (Feb. 7, 2018), https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data (explaining that it can be "any information that is clearly about a particular person").

76. *See* Penny Crosman, *Code Names and Flowers: Rabobank's Novel Approach to Customer Data*, AM. BANKER, July 23, 2018 [hereinafter *Code Names*], (commenting that while banking institutions will likely increasingly use pseudonymisation for privacy purposes, it is "important to still keep in mind that pseudonymized data remains subject to the GDPR.").

77. *GDPR*, *supra* note 8, at art. 4(1).

78. *GDPR*, *supra* note 8, at art. 4(1).

79. INFO. COMMISSIONER'S OFF., WHAT IS PERSONAL DATA?, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.

80. *See id.* ("You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example as a result of technological developments . . . .").

81. *See id.* ("In some circumstances there may be a slight hypothetical possibility that someone might be able to reconstruct the data in such a way that identifies the individual. However, this is not necessary sufficient to make the individual identifiable in terms of GDPR. You must consider all the factors at stake.").

82. *Code Names*, *supra* note 76.

protection for consumers' data in the event of a breach.[83] Also, unlike encryption or anonymization, pseudonyms retain the data's usefulness, preserving it for app testing and analytics.[84]

2. Personally Identifying Information That Monitors Behavior

Many banks are turning to biometric data to fight fraud, but data that tracks ongoing behavior of EU data subjects is by itself enough to establish GDPR jurisdictional reach.[85] In particular, the Commission was concerned with data processing that tracks and profiles natural persons for the purposes of "analysing or predicting her or his personal preferences, behaviors, and attitudes."[86]

GDPR concerns regarding predictive behavior data impact banks because many financial institutions are at the forefront of developing and using technology that stores and processes vast amounts of customers' biometric data.[87] Beyond cookies used for advertising purposes, the data-harvesting banks are undertaking is extraordinarily detailed and complex, "amassing tens of millions of profiles that can identify customers by how they touch, hold and tap their devices."[88] These programs can record and differentiate between thousands of gestures, methods, and idiosyncrasies as people tap, swipe, and scroll.[89] The technology detects fraud with 99%

83. *See* C*ode Names*, *supra* note 76 (suggesting that banks will use pseudonymisation more often post-GDPR).

84. *See id.* ("If you start with pseudonymisation, you can retain 100% of the data utility.").

85. *See GDPR, supra* note 8, at Recital 24 ("The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behavior of such data subjects in so far as their behavior takes place within the Union.").

86. *Id.*

87. *See* Karl Flinders, *Mastercard Sets Biometric ID Deadline for Banks,* COMPUTER WKLY. (Jan. 23, 2018), https://www.computerweekly.com/news/252433622/Mastercard-sets-biometric-ID-deadline-for-banks (discussing that banks that accept Mastercard payments will have to support bioID mechanisms, and that 92% of banking professionals want to introduce biometric identification methods; beyond that, very few banks disclose to users that they perform this tracking, which violates the consent requirements of GDPR).

88. *See* Cowley, *supra* note 2 ("The way you press, scroll and type on a phone screen or keyboard can be as unique as your fingerprints or facial features.").

89. *See id.* (discussing that "identity is the ultimate digital currency, and it's being weaponized at an industrial scale," making bioID protections all the more important).

accuracy[90] but can also serve other purposes.[91] For example, the technology can sometimes detect medical conditions, such as if a customer with a once-steady hand develops a tremor.[92]

This technology is quickly becoming the standard of identification technologies among U.S. banks.[93] American Express invested in the technology and has begun using it on new account applications.[94] Mastercard acquired a competitor technology last year.[95] IBM has built behavioral biometrics into the security software it sells to banks.[96] This trend raises GDPR concerns because inadequate protections for this biometric data could result in nearly irreversible identity theft.[97] In light of this concern, banks risk losing the ability to develop this technology and to store the resulting data logs under the principle of data minimization.[98] If there is another identification method that is just as effective for a given purpose but that results in less sensitive data collection and processing,

90. *See id.* (using an example of a bank utilizing the software to recognize that a customer had used a mouse's scroll wheel for the first time, which raised alarm bells, stopping cash from leaving the account—after investigation, it was revealed that the account had been hacked).

91. *See* Cowley, *supra* note 2; *see also* Rachel Minter, *The Informatization of the Body: What Biometric Technology Could Reveal to Employers About Current and Potential Medical Conditions,* A.B.A. (Apr. 7, 2011), https://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2011/eeo/014.authcheckdam.pdf (discussing privacy issues around the health data revealed through biometric identification processes).

92. *Id.*

93. *See A New Definition of Security. Biometrics In Digital Banking,* LIVE BANK (Feb. 20, 2018) https://livebank24.com/blog/biometrics-in-digital-banking/ ("As research and development of biometric technologies progresses, more and more banks jumped on the bandwagon.").

94. *See* Cowley, supra note 2 (discussing how banks are embracing biometric ID technologies); *see also* Mike Faden, *Biometrics' Growing Role in Payment Services,* AM. EXPRESS, https://www.americanexpress.com/us/content/foreign-exchange/articles/use-of-biometrics-for-payment-services/ (last visited Jan. 9, 2019) (discussing the growth of biometric identification in payment services).

95. *See* Cowley, *supra* note 2.

96. *See* Cowley, *supra* note 2.

97. *See* Daniel Uria, All *4 Major U.S. Credit Cards Ditch Signatures, with Eye on Biometrics,* UPI (Apr. 30, 2018), https://www.upi.com/All-4-major-US-credit-cards-ditch-signatures-with-eye-on-biometrics/4711523330286/ (noting that "any compromise of such a [biometric identification] database is essentially irreversible for a whole human lifetime: no one can change their genetic data or fingerprints in response to a leak," and raising the point that it is fairly easy for a motivated actor to take a high resolution photo of a person or to lift a fingerprint from something the person touches).

98. *See* INFO. COMMISSIONER'S OFF., PRINCIPLE (C): DATA MINIMISATION, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ [hereinafter Principle (c)] ("[P]ersonal data shall be. . . limited to what is necessary in relation to the purposes for which they are processed.").

then banks are obligated to use that method.[99] Under this requirement, regulators may study the relative efficacy of processing biometric data for fraud prevention purposes compared to other methods, such as alpha-numeric passwords and two-factor authentication, and conclude that the risk of processing biometric data outweighs the fraud-prevention benefits.[100] Some companies are hedging against the potentially catastrophic risk of disclosure of biometric data by anonymizing the data, but that gold standard of security may have a counterproductive effect on the usefulness of the data, as discussed below.[101]

The only way for banks to be sure that they do not need to comply with GDPR if they have identifiable data subjects in the E.U. is to anonymize the subjects' data.[102] However, banks will not practically be able to rely on anonymization to ease their compliance obligations because anonymization tends to render data unusable for analytical purposes.[103] Smaller banks that are unlikely to be using large quantities of biometric data may want to anonymize most of their data, especially when it is being stored and not being processed ("at rest"), for ease of compliance concerns. However, these banks will need to have a compliance plan prepared upon de-anonymization and processing if needed for discrete purposes, such as when a consumer applies for a new product, like a mortgage. Because of the difficulty in using anonymized data, encryption at

99. *See id.* (discussing the obligation to only collect personal data actually needed for specified purposes); EUR. COMM'N, WHEN CAN PERSONAL DATA BE PROCESSED?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en.

100. *See* EUR. COMM'N, WHEN CAN PERSONAL DATA BE PROCESSED?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en ("Your company/organisation may legitimately process personal data for that purpose, only if the least intrusive method is chosen as regards the privacy and data protection rights of [the data subjects] . . . .").

101. *See Privacy Policy,* BIOID, https://www.bioid.com/privacy-policy/ (last visited Jan. 9, 2019) (publishing the Privacy Policy of a service provider of biometric identification which includes provisions regarding anonymization); *see also Code Names*, *supra* note 76 (pointing out the relative uselessness of anonymized data).

102. *GDPR*, *supra* note 8, Recital 26 ("The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.").

103. *See Code Names*, *supra* note 76 (advocating for pseudonymisation over anonymization, and commenting that "there's no linkability, so no analytics can be run on it; trends and patterns can't be identified").

rest and pseudonymisation are likely a bank's best protocols for balancing GDPR compliance with security and usability concerns.

III. DATA MINIMIZATION

The overarching principle that emerges from GDPR is that institutions can only collect and process data if such data is necessary for one of a few permissible purposes.[104] Fortunately, the word "necessary" is typically interpreted very broadly under GDPR requirements.[105] Essentially, as long as banks can articulate why the results of the processing cannot reasonably be achieved without the processing, the processing will be deemed necessary.[106] Beyond that, banks may also process for subsequent purposes so long as that processing is compatible with the initial purpose.[107] Compatibility is determined by taking into account various elements such as the context, the nature of the data, the possible consequences for the data subject, and appropriate guarantees, such as encryption and pseudonymisation.[108] The practical effect of these provisions is that with a well-written privacy policy that lists all possible, permissible purposes and outlines appropriate protections, banks may not actually need to change the way they process data at all.[109]

To revise a privacy policy to aid GDPR compliance, banks should write their terms with as many potential purposes as possible, not just a

104. *GDPR*, *supra* note 8, Article 25(2) ("The controller shall implement appropriate technical and organizational measures that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.").

105. *See* INFO. COMMISSIONER'S OFF., LAWFUL BASIS FOR PROCESSING, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ ("If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.")

106. *See id.* (providing a guide for organizations in interpreting GDPR).

107. *See Data Protection—Impacts of GDPR in the Banking & Financial Sectors*, JOYN (June 2017) https://www.joynlegal.be/images/actualite/Newsletter%20GDPR%20-%20JOYN%20Legal.PDF ("Further processing for other purposes than the initial purposes shall be compatible with the latter.").

108. *See id.* (discussing the factors that may be relevant to necessity and proper purposes for processing).

109. BANK OF AM. MERRILL LYNCH, GENERAL DATA PROTECTION REGULATION 2018: CHANGES TO COMMERCIAL CARD CONTRACTS, https://www.bofaml.com/content/dam/boamlimages/documents/articles/ID18_0208/BofAML_GDPR_Changes_to_Contractual_Documentation_FAQs_March_2018.pdf (last visited Jan. 9, 2019).

blanket statement such as "to provide the services."[110] For example, a bank could state that "we process your data in order to provide the financial services requested, for everyday business purposes, for our marketing purposes, for joint marketing with other financial companies, to provide information on other services which you may be interested in, to prevent fraud and abuse of the financial system, and to comply with legal obligations."[111] Even though GDPR exempts processing for fraud prevention purposes from the data subject's right to erasure, and fraud prevention is a legitimate goal for processing, it is important to also specify that purpose for every piece of data that could rationally be related to that goal because it is likely that the regulators will strongly favor the data subjects.[112]

A. Consent as a Legal Basis for Processing

While there are six permissible justifications for processing PII,[113] this Note focuses on consent, which has received the most attention in the media and is perhaps the biggest departure from previous requirements.[114]

The ability to demonstrate that the data subject has consented to the processing of their data may sound easy, but it may in fact be the biggest challenge of GDPR compliance.[115] Because of these new

110. *See Data Protection – Impacts of GDPR in the Banking & Financial Sectors*, *supra* note 107 (providing suggestions for drafting notices as broadly as possible).

111. *Id.*

112. *See* Daphne Keller, *The "Right to be Forgotten" and National Laws Under the GDPR,"* CTR. FOR INTERNET AND SOC'Y (Apr. 27, 2017), http://cyberlaw.stanford.edu/blog/2017/04/%E2%80%9Cright-be-forgotten%E2%80%9D-and-national-laws-under-gdpr ("[GDPR] appears to strongly tilt the playing field in favor of [right to be forgotten] requests.").

113. *See* INFO. COMMISSIONER'S OFF., LAWFUL BASIS FOR PROCESSING, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (last visited Jan. 9, 2019) (laying out legitimate justifications of: (1) the processing is performed with clear consent to process for a particular purpose; (2) the processing is necessary to fulfill a contract with the data subject; (3) the processing is necessary to comply with the law; (4) the processing is necessary to save someone's life; (5) the processing is in the public interest or pursuant to a government function; (6) there is a legitimate interest in the processing which overrides the individual's interest in their personal data).

114. *See* Suman Chattacharyya, *How US Banks are Preparing for the GDPR*, TEARSHEET (Apr. 16, 2018), https://www.tearsheet.co/data/how-us-banks-are-preparing-for-the-gdpr (discussing that the consent cannot be the typical click-wrap or "silence is consent" approach that many banks are used to).

115. *Id.*

requirements, banks must put new consent protocols in place and go back to confirm subjects' consent instead of grandfathering in their current data subjects.[116]

Under GDPR, consent "requires customers to be made fully aware, in a clear, concise and transparent fashion, of how their personal data will be used and by whom."[117] Essentially, it must be: (1) separate;[118] (2) in clear and plain language;[119] (3) as easy to withdraw as it is to give;[120] and (4) not a required contractual condition if it the provision is not necessary for completing the processing.[121]

These elements raise a number of considerations. Because of the separation requirement, banks cannot include a laundry-list of permissions deep within the terms and conditions.[122] Pre-ticked boxes will not suffice; consent for GDPR purposes requires affirmative action.[123] If banks are processing data for multiple purposes, consent must be given for all of the purposes.[124] As one professional lamented, "the customer experience is going to be potentially dramatically changed by these regulations."[125] "It's almost as if the governments are dictating the enterprise design or system design or consumer experience."[126]

For example, banks are increasingly adopting Apple's Face ID and other facial recognition technologies "to let people log into mobile banking with a selfie."[127] This technology and other bioID programs create consent issues if banks are not transparent with customers about what

116. *Id.*

117. *Open Banking and PSD2: A Revolution in the Provision of Retail Banking Services*, 6 J. INT'L BANK. & FIN. L. 395 (2018).

118. *GDPR*, *supra* note 8, Article 7(2).

119. *GDPR*, *supra* note 8, Article 7(2).

120. *GDPR*, *supra* note 8, Article 7(3).

121. *GDPR*, *supra* note 8, Article 7(4).

122. *See* CNIL, *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (discussing Google's lack of valid consent regarding ads personalization, because information was not easily accessible for users and was spread out across several pages).

123. INTERSOFT CONSULTING, GDPR CONSENT, https://gdpr-info.eu/issues/consent/ (last visited Jan. 9, 2019).

124. *Id.*

125. *How Much Will the GDPR Change Consumer Technology?*, RECORDER (CAL.) (Dec. 27, 2017) (discussing how the consent requirement will change design and user experience).

126. *Id.*

127. *See* Penny Crosman, *Facing up to Bias in Facial Recognition,* AM. BANKER, May 29, 2018, https://www.americanbanker.com/news/facing-up-to-bias-in-facial-recognition [hereinafter *Facing up to Bias*] (discussing the flaws in this technology that make it secure for white men but dangerously insecure for minorities and women).

data is being stored and used, and if the customer cannot clearly and easily find the specific purposes for which the banks are using the data.[128] For example, FaceID data is shared with third party developers and used for marketing and advertising purposes, not just as a modern password.[129] This use could violate data subjects' rights in the exact way the regulators were targeting if customers have not affirmatively consented to their biometric data being used in this way, because the bank would have to argue that using biometric data for advertising purposes is necessary for a permissible purpose and therefore justified, even when compared to other possible sources of data that could be used for advertising and marketing.[130]

Furthermore, the open question about whether biometric ID is afforded the same Fifth Amendment protections as traditional passwords and PINs, subject FaceID and other biometric IDs to other risk of which many consumers may be unaware.[131] The potential consequences of this, along with the potential consequences of a breach, mean that banks should conservatively choose to allow people to opt in to their specialized fraud prevention programs via a special opt-in page, instead of through the standard terms.[132] Some banks already complete a similar process for location tracking; however, the tracking requires phone permissions that are already visible to consumers.[133] For more sophisticated technology that tracks without any notifications from the customer's phone, banks should be cautious and obtain consent, especially in light of the Commission's avowed mission to prevent undisclosed data accumulation.[134]

128. *See* CNIL, *supra* note 122 (discussing Google's lack of transparency with consumers which warranted an enforcement action).

129. *See* Christina Binnington, *Apple Plans to Share Some Data That the iPhone X Collects About Your Face. That's a Huge Worry,* SLATE (Nov. 2, 2017), http://www.slate.com/blogs/future_tense/2017/11/02/apple_plans_to_share_some_iphone_x_face_id_data_uh_oh.html (pointing out that third party developers will be able to access FaceID data).

130. *See* Luke Irwin, *GDPR: Things to consider when processing biometric data*, IT GOVERNANCE (Sept. 15, 2017) https://www.itgovernance.eu/blog/en/gdpr-things-to-consider-when-processing-biometric-data

131. *See* Binnington*, supra note 115.* ("[C]ourts could compel an individual unlock their phone using biometrics, as 'attributes of the body' are not protected under the Fifth Amendment.").

132. *See* CNIL, *supra* note 122 (discussing Google's fines for consent-related noncompliance).

133. *See* Victor Luckerson, *Your Bank Wants to Know Where You Are,* TIME (March 4, 2016), http://time.com/4247847/banks-tracking-cell-phone-fraud/ (pointing out that a banking location monitoring program will be opt-in).

134. *See* A NEW ERA, *supra* note 3 (highlighting the goal of preventing issues like those revealed in the Facebook/Cambridge Analytica scandal).

Because of the Commission's mission in this regard, the area of consent surrounding biometric tracking and identification is probably the area of the financial industry that is most likely to see a GDPR enforcement action.[135]

B. Rights of Data Subjects Over their Data

All of the provisions within GDPR are promulgated in order to support the five enumerated rights that data subjects have over their data, namely: (1) the right to use; (2) the right to erasure; (3) the right to portability; (4) the right to edit; and (5) the right to restrict.[136] The right to erasure and the right to portability have perhaps the most interesting implications for banks.[137] Like most U.S. companies, banks are not used to responding to deletion requests, but unlike other institutions, banks are especially ill-equipped to navigate the exercise of a deletion request because of the countervailing interests of accounting needs, prevention of money laundering, taxation, and other general banking laws.[138] Because of this, most U.S. banks will need to undergo a deeper data mapping project to respond to these requests than other institutions.[139] The response to a deletion request cannot be simply "no"; rather, banks must provide customers with an explanation of all of the information they hold on the individual, why they have it, and why they must retain it.[140] This

135. *See* Danny Ross, *Processing biometric data? Be careful, under the GDPR,* THE PRIVACY ADVISOR (Oct. 31, 2017), https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/ ("The evolving nature of biometric technology, the inherent uncertainties associated with the GDPR's treatment of biometric data, and the expected divergence of Member States' approaches to biometric data all warrant the attention and caution of data controllers.").

136. *See id.* (providing a brief overview of the rights and obligations granted and imposed by GDPR).

137. *See, e.g.,* William Barry, *Financial Data: A Compliance Conundrum for Financial Institutions: U.S. Anti-Money Laundering Initiatives and the Forthcoming EU General Data Protection Regulation*, BLOOMBERG (Dec. 11, 2017), https://www.bna.com/compliance-conundrum-financial-n73014473009/ (discussing how GDPR fundamentally conflicts U.S. AML/CTF compliance practices).

138. *See GDPR Deep Dive—How to Implement the 'Right to be Forgotten'*, BANKINGHUB (Nov. 15, 2017), https://www.bankinghub.eu/banking/finance-risk/gdpr-deep-dive-implement-right-forgotten ("[F]or financial institutions with complex interrelated systems, timely GDPR compliance will pose a major challenge."); *see also* Barry, supra note 137 (discussing issues relating to U.S. AML/CTF compliance).

139. *See id.* ("[W]e strongly advise financial institutions to implement their tactical response to GDPR with the roadmap for future development of the organization and IT-landscape in mind.").

140. *See Right of access,* INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-

requirement is familiar to American lawyers as the right to be forgotten; however, most existing stored data mapping and source classification will not be comprehensive enough to satisfy GDPR regulators.[141] Instead, banks should update their data maps with information on when the permissible purpose for retention will expire, and put processes in place to facilitate deletion after the lawful purpose expires.[142] Then, they should follow up with the data subject confirming that all data not required to be retained has been deleted (such as marketing, advertising, correspondence, and publicly available information), and explaining what is being retained and why the bank has the right to do so.[143]

Another significant new right is the right to portability.[144] Data subjects must be able to easily access copies of their personal data in a usable format that can be transmitted electronically to other processing systems.[145] This allows individuals to easily switch between different service providers, and is analogous to the principles of Open Banking, where "U.S. bankers are watching their European counterparts, anticipating a day they themselves lose their monopoly on customer data to merchants and retailers like Amazon (with customers' permission)."[146] That day has come with GDPR compliance. Banks will need to not only provide customers with their data to give to another financial provider, but also facilitate the transfer themselves if the customer asks, which can

gdpr/individual-rights/right-of-access/ (last visited Jan. 9, 2019) ("You must inform the individual without undue delay and within one month of receipt of the request . . . the reasons you are not taking action; their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy.").

141. *See* Dan Clark, *Data Mapping May be the Hardest Part of GDPR Compliance,* CORP. COUNS. (Aug. 15, 2018), https://www.law.com/corpcounsel/2018/08/15/data-mapping-may-be-the-hardest-part-of-gdpr-compliance/ (discussing how much of a challenge data mapping for GDPR purposes can be, and how it may be advertised as a competitive advantage in the future).

142. *See* Rita Heimes, *Top 10 Operational Responses to the GDPR – Part 5: Preparing and implementing data-retention and record-keeping policies and systems,* IAPP (Feb. 26, 2018), https://iapp.org/news/a/top-10-operational-responses-to-the-gdpr-part-5-preparing-and-implementing-data-retention-and-record-keeping-policies-and-systems/ (discussing the design and implementation of data retention policies and data destruction policies).

143. *See id.* (discussing general methods of facilitating a data deletion request, including a CRM functionality of overwriting fields with anonymized text).

144. A NEW ERA, *supra* note 3.

145. *See* INFO. COMMISSIONER'S OFF., RIGHT TO DATA PORTABILITY, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/ (last visited Jan. 9, 2019) [hereinafter RIGHT TO DATA PORTABILITY] ("[P]rovide the personal data in a format that is: structured; commonly used; and machine-readable.").

146. *See* Chattacharyya, *supra* note 114 (discussing the intersection of GDPR and Open Banking).

bring a landmine of possible compliance pitfalls and requires compliance with a set of model data transfer clauses.[147] Beyond transfers, the data given to the subjects must be usable, requiring the data be put in a format that is readable by others, or requiring that the banks give interpretations of how to read the data.[148]

C. Privacy by Design

In navigating GDPR, banks should look to the principles of "Privacy by Design," a central tenet of GDPR.[149] Privacy by Design is the idea that engineering processes and the creation of new products and platforms should center around data protection through the technology's design.[150] Creating a comprehensive scheme will be easier for smaller banks that do not have vast amounts of older systems and data to re-organize, but may also pose a challenge for developers who are unaccustomed to writing code that is security-centric and helps facilitate requests by data subjects.[151] Banks of all sizes should have conversations across all teams to understand what personal data they have, where it is stored, what they use it for, and who it is shared with.[152] For example, a Marketing team may intuitively understand that leads are PII, but may not realize that aggregated data is likely not truly anonymized, and thus contains PII

147. *See* RIGHT TO DATA PORTABILITY, *supra* note 145 ("The right to data portability entitles an individual to: receive a copy of their personal data; and/or have their personal data transmitted from one controller to another controller.").

148. *See* RIGHT TO DATA PORTABILITY, *supra* note 145 (moving the data must not affect its usability).

149. *See* ICO, DATA PROTECTION BY DESIGN AND DEFAULT, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (last visited Jan. 9, 2019) ("The GDPR requires you to put in place appropriate technical and organizational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and default.'").

150. *See id.* ("[Y]ou have to integrate or 'bake in' data protection into your processing activities and business practices . . . .").

151. *See id.* ([W]hen considering what products and services you need for your processing, you should look to choose those where the designers and developers have taken data protection into account . . . If you are a developer or designer of products, services and applications . . . if you design these products with data protection in mind, you may be in a better position.").

152. *See* Joseph Facciponti & Katherine McGrail, *GDPR Is Here—What if You Didn't Prepare?* LAW 360 (May 24, 2018), https://www.mmlawus.com/newsitem/pdf/GDPR_Is_Here_-_What_If_You_Didnt_Prepare_-6492704862338379015.pdf (advocating "know your data," and undergoing a data mapping exercise to navigate the organizations' cross-team data flow).

that falls under GDPR's protections.[153] Likewise, Customer Service may recognize that a customer's name and PIN given on a phone call is protected but not realize that the randomly generated number associated with the case number is also protected. Once these conversations throughout the institution's teams are carried out, a giant map of all PII can be constructed, and conversations can begin about why all of the data is being held and processed.[154] In order to facilitate requests from data subjects, "banks need to be able to reconcile how the data flows between all these different databases, even though they were made in different times, they may have different forms [and] the data may be called something different."[155] This approach is important because it will be nearly impossible to comply with GDPR retrospectively. Instead, it is important to develop documentation of what data a bank holds on a subject, why it has it, and how long they can legally retain the data following a deletion request.[156] This mapping may take years and millions of dollars to carry out.[157] If a bank waits for requests to pile up or for an enforcement action to begin, it will be difficult, or potentially impossible, to retroactively respond in satisfactory manner.[158]

Most banks are struggling with this process.[159] Seventy percent of banks stated moderate confidence that they can find about fifty percent of instances of personal data in their systems in the event of an individual requesting deletion.[160] If banks cannot complete data inventory in a way

153. *See* Kate Kaye, *Research: Your Aggregated Consumer Data May Not be Secure,* ADAGE (May 18, 2017), https://adage.com/article/privacy-and-regulation/aggregating-data-guard-privacy-vc-s/309068/ (shedding light on how individuals can still be identified through aggregated data).

154. *See* Chattacharyya, *supra* note 114 (discussing data mapping as a starting point in a GDPR compliance plan).

155. Jingnan Huo, *EU's New Data Privacy Law Creates Headaches for U.S. Banks*, AM. BANKER 1, 3, Sept. 20, 2017, https://www.americanbanker.com/news/eus-new-data-privacy-law-creates-headaches-for-us-banks (discussing that GDPR "requires business practices that banks don't have in the U.S.," such as a way of providing clients with full access to data about themselves).

156. *See* Huo, *supra* note 155 ("GDPR drives companies to develop documentation ahead of time.").

157. *See* Clint Boulton, *U.S. Companies Spending Millions to Satisfy Europe's GDPR*, C.I.O. (Jan. 26, 2017, 9:56 AM), https://www.cio.com/article/3161920/privacy/article.html (describing compliance as "agonizing" and citing that 68% of U.S. multinational companies are spending more than a million dollars on GDPR compliance).

158. *See* Huo, *supra* note 155 ("GDPR drives companies to develop documentation ahead of time.").

159. Duncan Brown, *Ready or Not? GDPR Maturity Across Vertical Industries*, INT'L DATA CORP. (Apr. 2, 2017).

160. *Id.*

that facilitates such requests, they face the risk of being targeted with an enforcement action.[161]

Some banks are addressing their struggle to comply by conducting Data Protection Impact Assessments ("DPIAs") and by hiring Data Protection Officers ("DPOs") to oversee their implementation.[162] Especially during the early stages of road mapping a path to compliance, banks are discovering that the "best practice will be for banks to nominate qualified persons to assume the responsibility of undertaking a DPIA."[163] Beyond this voluntary hiring trend, DPIAs are mandatory when processing is likely to result in a high risk to a subject's rights, such as where a bank screens customers against a credit reference database or where banks are using automated decision making processes.[164]

Practically speaking, the flow of a bank's DPIA should be carried out as follows. First, the bank should identify broadly the need for the DPIA.[165] Why is it being carried out?[166] What processing or project is suspected to be especially problematic?[167] Next, the bank should describe in detail how the information will be processed.[168] How will it be sourced, collected, stored, used, deleted?[169] Who will have access to the data? How and where will it flow?[170] Based on the description of processing, the bank will have a clearer picture of the scope of the data.[171] How many data subjects does it implicate?[172] Where will the data subjects likely be from, geographically?[173] What type of data is the bank

161. *See* Huo, *supra* note 155 ("There's real enforcement risk . . . .").

162. FENERGO, GDPR: GAME CHANGER FOR MANAGING DATA & REGULATORY COMPLIANCE 1, 11 (Sept. 2017), https://www.fenergo.com/resources/whitepapers/gdpr-managing-data-protection.html

163. *Id.*

164. *See The General Data Protection Regulation*, 6 COMPUTER LAW § 51.04 (Aug. 25, 2018) (discussing that even where controllers and processors have outsourced the role of DPO, they maintain responsibility for the actions of the DPO).

165. *See* INFO. COMMISSIONER'S OFF., HOW DO WE CARRY OUT A DPIA?, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-carry-out-a-dpia/ (last visited Jan. 9, 2019) [hereinafter *How do we carry out a DPIA*] (describing step one as deciding whether a DPIA is necessary, and recommending erring on the side of caution).

166. *Id.*

167. *Id.*

168. *See id.* (listing a number of factors having to do with the nature of the processing that is to be carried out).

169. *Id.*

170. *Id.*

171. *How do we carry out a DPIA, supra* note 165.

172. *How do we carry out a DPIA, supra* note 165.

173. *How do we carry out a DPIA, supra* note 165.

collecting, about whom, and does it include those individuals' sensitive or biometric information?[174] Based on the breadth of the scope, the bank should articulate why it needs the data.[175] Could that end goal be achieved with less data, or less biometric data?[176] What are the relative benefits to the bank and risks to the data subject of this processing?[177] With those answers in mind, the bank can translate the information into legal bases for processing, and document a legal purpose and justification for each instance of data gathering and processing.[178] Finally, in a global sense, the risk management team and perhaps the C-Suite can discuss the biggest source of risk to the data, along with the likelihood of the harm and likely severity of the harm, and come to a business decision on the bank's chosen risk profile.[179] Going through this process for each area of high impact processing will force banks to develop a compliance plan and map for responding to requests from the ground up.[180]

IV. PENALTIES FOR NONCOMPLIANCE

The penalties for non-compliance are perhaps the most striking aspect of GDPR.[181] European Commission regulators can carry out investigations, order entities to take remedial measures for deficiencies, and impose administrative fines of up to EUR 20m or four percent of the total worldwide annual revenue (whichever is higher), by either reacting to complaints or through proactively investigating the most glaring violations.[182] Individual Member States can also impose additional penalties

174. *How do we carry out a DPIA, supra* note 165.

175. *See How do we carry out a DPIA, supra* note 165 ("[I]s there any other reasonable way to achieve the same result?").

176. *How do we carry out a DPIA, supra* note 165.

177. *How do we carry out a DPIA, supra* note 165.

178. *See* Alison Cregeen*, A Practical Guide to Data Mapping for GDPR Compliance,* PRICEWATERHOUSECOOPERS (Mar. 6, 2018), https://www.pwc.com/im/en/media-room/articles/a-practical-guide-to-data-mapping-gdpr.html (discussing how the process forms the basis of documenting the lawful bases for processing).

179. *See* Danielle Bauer, *6 Steps to GDPR Implementation*, RISK MGMT. (last visited Jan. 9, 2019), http://www.rmmagazine.com/2018/04/02/6-steps-to-gdpr-implementation/ (discussing using the process as a risk management protocol).

180. *See id.* (discussing developing a compliance plan).

181. *See Fines and Penalties*, GDPR EU.ORG (last visited Jan. 9, 2019), https://www.gdpreu.org/compliance/fines-and-penalties/ (discussing the plain language of the regulation and describing how high the fines for noncompliance are).

182. *See id.* (discussing the plain language of the regulation); *see also* Bernard Marr, *GDPR: The Biggest Data Breaches and the Shocking Fines (That Would Have Been),* FORBES (June 11, 2018), https://www.forbes.com/sites/bernardmarr/2018/06/11/gdpr-the-biggest-data-breaches-and-the-shocking-fines-that-would-have-been/#6d9642326c10 (discussing

(including criminal sanctions).[183] Data subjects can bring private lawsuits to collect damages for harm resulting from violation of their rights in addition to the regulatory fines.[184] Beyond this, large institutions are worried that GDPR could allow for class-action liability.[185] GDPR also provides that "the data subject shall have the right to mandate a not-for-profit body, organization or association . . . to lodge the complaint on his or her behalf."[186] Some are concerned that non-profits will be formed so that "Europeans will in future be able to bring US-style class actions for (alleged) privacy violations, instead of having to sue individually and expensively."[187] In fact, the first such group has already formed, purportedly ready and willing to litigate on behalf of large groups of consumers whose rights under GDPR have been violated.[188] This potential civil liability, combined with the regulatory fines, mean that a GDPR enforcement action and subsequent suit could be very costly for even the largest institutions.[189]

---

how the 2014 Yahoo breach could have resulted in up to $160 million in fines under GDPR); Douglas Busvine et. al., *European Regulators: We're Not Ready for New Privacy Law,* REUTERS (May 8, 2018), https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X (discussing that the majority of GDPR enforcement bodies will not proactively investigate compliance due to lack of resources).

183. *See Fines and Penalties*, *supra* note 181; *see also* DETLEV GABEL & TIM HICKMAN, WHITE & CASE, CHAPTER 16: REMEDIES AND SANCTIONS—UNLOCKING THE EU GENERAL DATA PROTECTION REGULATION (Jul. 22, 2016) https://www.whitecase.com/publications/article/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection (discussing the power of individual Member States to impose criminal sanctions).

184. *See* John Patzakis, *GDPR Provides a Private Right of Action. Here's Why That's Important* (Feb. 28, 2018), https://blog.x1discovery.com/2018/02/28/gdpr-provides-a-private-right-of-action-heres-why-thats-important/.

185. *See* Bryan Betts, *GDPR's Latest Gift? Class Action Privacy Cases*, COMPUTER WKLY. (Jan. 29, 2018), https://www.computerweekly.com/blog/Write-side-up-by-Freeform-Dynamics/GDPRs-latest-gift-Class-action-privacy-cases (calling the class action a "logical extension" of Article 80).

186. *GDPR, supra* note 8, art. 80.

187. *See* Betts, *supra* note 185 (calling the class action a "logical extension" of Article 80).

188. *See GDPR: Noyb.eu Filed Four Complaints Over "Forced Consent" Against Google, Instagram, WhatsApp, and Facebook*, NOYB (May 25, 2018), https://noyb.eu/ (publicizing four class action lawsuits brought by a privacy advocate filed against Google, Instagram, WhatsApp, and Facebook under consent-based GDPR causes of action); *see also* Derek Scally, *Max Schrems Files First Cases Under GDPR Against Facebook and Google: European Data Protection Bodies Vow to Work with Irish Colleagues on Complaints,* IRISH TIMES (May 25, 2018), https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177 (discussing two complaints based on inadequate consent under GDPR).

189. *See* Betts, *supra* note 185 (discussing class action liability); *see also Fines and Penalties*, supra note 172 (discussing the fines and penalties at stake); *see also* Gabel, *supra* note

While institutions that have previously been controllers of E.U. data may be accustomed to some risk exposure with regard to that data, especially from the previous Directive 95/46/EC, GDPR's potential liability is unique in that it applies to both controllers and processors of data.[190] Therefore, even financial institutions that operate solely on a business-to-business basis may be exposed to the same liability that their customers are exposed to (in their business to consumer roles), by nature of processing their business customers' consumers' information.[191] Furthermore, for GDPR causes of action, there is a reversed burden of proof.[192] Instead of the claimant needing to prove a violation, the defendant institution will need to prove that it acted in compliance with GDPR.[193] This emphasizes the need to develop a data map and articulate legal bases for processing up front, instead of reacting after an action is brought.

V. CONCLUSION AND RECOMMENDATIONS

In light of the large penalties at stake under GDPR, larger banks should conservatively interpret the ambiguities of the GDPR, including by implementing a compliance plan that affords GDPR protections to all person who are physically present in the Union.[194] Smaller banks may be better off adopting a wait and see approach, while facilitating compliance for citizens and long-term residents of the EU.[195] For banks across the spectrum, it is essential to be conducting a sweeping inventory of

183 (discussing possible criminal sanctions); *see also* Patzakis *supra* note 184 (discussing potential private rights of action).

190. *See* Martin Strauch, *How Article 82 of the GDPR Has Revised the Rules on Liability, Compensation Claims, and Class Actions when Data Breaches Occur in Europe,* HOGAN LOVELLS PUBLICATIONS (July 24, 2018), https://www.hoganlovells.com/en/publications/how-article-82-of-the-gdpr-has-revised-the-rules-on-liability-compensation-claims-and-class-actions-when-data-breaches-occur-in-europe.

191. *See id.* ("a processor might actually become subject to a direct claim by a data subject, even though the processor might be a company that is only acting in a B2B (business-to-business) setting . . . .").

192. *See id.* (discussing "four major changes to the way data breaches are addressed . . ." including "a reversed burden of proof . . . .").

193. *See id.* (pointing out GDPR's reversed burden of proof).

194. *See* Miller, *supra* note 48 ("'GDPR has made people wake up to the fact of accountability' . . . organisations are taking [this]seriously.").

195. *See* Crosman, *supra* note 10 ("I don't know that if I had one European customer I would go through the effort of complying with GDPR . . . [b]ut technically, you would be subject to GDPR.").

personal data and the purposes for which it is collected and stored.[196] With the amount of data most banks are collecting, storing, and processing, banks should have a plan in place for recognizing each instance of PII across the system, and to be able to give a timely response to a data subject or regulator who inquires about it.[197] To jumpstart that effort, both at the beginning of compliance and at the start of each roll-out of a new product, banks should carry out at DPIA even if they are not required to under the law.[198] With the potential fines at stake and the trend around the world of more stringent privacy laws being passed, conducting a cross-team inventory and map of all data and thinking critically about why the data is needed can not only help aid compliance with GDPR, but also position the bank to be ready for the slew of hefty privacy laws getting proposed and passed around the world.[199]

LINDSAY A. SEVENTKO

196. *See* Facciponti, *supra* note 152 (advocating "know your data," and undergoing a data mapping exercise to navigate the organizations' cross-team data flow).

197. *See* Facciponti, *supra* note 152 (regarding the importance of data mapping).

198. *See GDPR: Game Changer for Managing Data & Regulatory Compliance*, *supra* note 151.

199. *See* Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html (discussing California's new privacy law); *see also* Saritha Rai, *India Weighs Comprehensive Data Privacy Bill, Similar to EU's GDPR,* INS. J. (July 31, 2018), https://www.insurancejournal.com/news/international/2018/07/31/496489.htm (discussing India's proposed privacy bill that would greatly affect U.S. technology companies); *see also* JESSICA TREVELLICK, KING & SPALDING, CANADA TO UPDATE DATA LAW TO GDPR STANDARD AS A MINIMUM, https://www.jdsupra.com/legalnews/canada-to-update-data-law-to-gdpr-16052/ (last visited Jan. 9, 2019) (discussing amendment's to PIPEDA that make it similar to GDPR); *see also* Drinker Biddle & Reath, *Brazil Adopts New Privacy Law Similar to GDPR,* LEXOLOGY (Aug. 28, 2018), https://www.lexology.com/library/detail.aspx?g=2b0a61cb-d3ed-4027-a00a-b697eb2df062 (pointing out the main tenets of Brazil's new privacy law mirror GDPR).