The Prospective Impact of the Global Data Protection Regulation on Entrepreneurship: A Roboadvisor Case Study

AMBER AUSLEY*

CONTENTS

I. INTRODUCTION ................................................................. 85
II. WHAT IS THE GDPR ............................................................... 87
III. WHAT IS ROBO-ADVISING? ...................................................... 92
IV. THE IMPACT OF THE PROVISIONS OF THE GDPR ON ROBOADVISORS 93
   A. General Overview ................................................................. 93
   B. The Right to Be Informed ...................................................... 98
   D. The Right of Rectification .................................................... 100
   E. The Right of Erasure ............................................................ 101
   F. The Right to Restrict Processing and the Right to Object .. 102
   G. The Right to Data Portability ................................................. 102
V. CONCLUSION ............................................................................. 103

I. INTRODUCTION

This paper begins by discussing the most important development in privacy in recent years, the Global Data Protection Regulation (“GDPR”), which went into effect on May 25, 2018.¹ The GDPR,

* J.D. Candidate, 2019, University of Pennsylvania Law School; B.A., 2016, University of Alabama. I owe my greatest thanks to Professor Tom Baker, for without his encouragement and diligent supervision, this piece would not have been possible; to Professors Christopher Yoo and Lauren Steinfeld, who originally sparked my interest for privacy law
although originating in the European Union (“EU”), will have a worldwide impact, and no doubt will influence virtually every startup in Silicon Valley. Understanding the complexities of the GDPR will be essential to survival as a company. This discussion will begin in Section II by specifically outlining what the GDPR is, whom it will impact, and the essential provisions that make the regulation so significant for companies worldwide. The section will explain the normative policy goals of the GDPR and the steps necessary for realizing them. Section III of this paper will then shift to discuss what a roboadvisor is and how roboadvisors are different from existing platforms for investment and the value-add that they purportedly provide to consumers. The section will discuss various forms of roboadvisors, with a more in-depth focus on investing roboadvisors. Section IV combines the discussions in the preceding sections to analyze the essential provisions of the GDPR and their subsequent regulatory impact on roboadvisors. This section will dissect the impact of the GDPR on investment roboadvisors specifically, but will be foundationally applicable to other forms of entrepreneurship and industries. It is important to note that this section relies on assumptions regarding the actual implementation and enforcement of these provisions, as the GDPR is still a developing regulation. The paper will then conclude with recommendations for roboadvisors and startups as they begin to address the massive regulation.

---


2 Roboadvisors could use algorithms to advise people about their “deposit accounts, home mortgages...all of the personal lines of insurance...and from the securities sector, mutual fund shares and other savings products regulated as securities.” Tom Baker & Benedict Dellaert, Regulating Robo Advice Across the Financial Services Industry, 103 Iowa L. Rev. 713, 721 (2017). However, this paper mostly focuses on investment roboadvisors due to the fact that they are currently the most widely used type of roboadvisor, and also rely on a larger amount of personal data to make recommendations. However, the impact of the GDPR on roboadvisors, as discussed in Section IV of the paper, will mostly be consistent among different types of roboadvisors. The focus is not necessarily what data are being used, but rather how they are being used. Investment roboadvisors provide the best in-depth analysis to serve as a guide for other types of roboadvisors.
II. WHAT IS THE GDPR

The EU recognizes that the protection of natural persons in relation to the processing of personal data is a fundamental right. In consideration of this fundamental human right, the EU notes that, “[r]apid technological developments and globalisation have brought new challenges for the protection of personal data.” The scale of collecting and sharing information has grown astronomically, particularly as a result of social media, and now public and private institutions have access to massive amounts of personal data whether they intended to or not. It is highly likely that consumers do not know how much information is collected on them and who is using it. Therefore, the EU has made it a priority to implement changes in the current privacy system to “facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations, while ensuring a high level of the protection of personal data.”

As a result, the GDPR could be the most substantial change to the international privacy regime to date. After more than four years of intense discussion and negotiations among EU member states, both the European Parliament and the European Council passed the resolution in April 2016. The GDPR came into force on May 25, 2018.

---

3 See Charter of Fundamental Rights of the European Union art. 8(1), 2012 O.J. (C 326) 397 [hereinafter Charter]; Consolidated Version of the Treaty on the Functioning of the European Union art. 16, 2012 (C 326) 55 [hereinafter TFEU] (providing that “everyone has the right to the protection of personal data concerning [him or her].”).

4 Regulation 2016/679, supra note 1 at 2.

5 The GDPR does not apply to information that is publicly provided by citizens, but does apply to the social media platforms that host and use this data. Chris Payne, GDPR & Personal Data in the Public Domain, INFINIGATE (May 30, 2018), https://blog.infinigate.co.uk/gdpr-personal-data-public-domain [https://perma.cc/U6BC-S5F].


7 Regulation 2016/679, supra note 1 at 2.

and will impact the EU and any company that deals with data of European citizens.9

Prior to the GDPR, the EU had the Data Protection Act.10 However, that agreement was not self-executing and required individual passage by the governing bodies of each member state.11 As a result, each country in the Union had disparate and complicated privacy provisions.12 It was immensely expensive for companies to comply with each different country’s inconsistent rules, and companies could be haphazard with their privacy compliance.13 The purpose of the GDPR, then, was to provide uniformity and certainty regarding data protection for citizens of the Union.14 As a result of harmonization, the GDPR is expected to save corporations a total of €2.3 billion annually.15

The GDPR is attracting so much attention because the applicable scope of the GDPR is incomparably broad. The rules apply both to organizations established in the EU, and also to non-EU controllers and processors if they have EU customers or monitor behavior that takes place in the EU.16 Therefore, even if a company reaches one EU customer or employs a single EU citizen, the company must be fully compliant with the GDPR in regard to that person’s data. In practice, this means that if a European citizen has the ability to log into a website (even from a US IP address), that company will be responsible for complying with the GDPR. In contrast, the most expansive US privacy regulation, HIPAA, is narrowly defined to only regulate

---

9 Regulation 2016/679, supra note 1 at 32-33, 87.


11 Id.

12 Id.

13 Id.

14 Regulation 2016/679, supra note 1, at 19.


16 Regulation 2016/679, supra note 1, at 32.
covered entities. 17 While HIPAA only impacts healthcare providers, health plans, and clearinghouses, the GDPR applies to basically any company in the world that has a website that collects cookies from users, provided that the website could be accessed by a European citizen.

A company could potentially avoid the reach of the GDPR if they found a mechanism for avoiding EU customers, although this situation will be rare. First, it may be more expensive for a company to find a way to screen out EU customers rather than comply with the regulation. Secondly, it seems nearly impossible to ensure that EU citizens are not interacting with the company at all, such as through a U.S. IP address. Even if a company could find a way to operate entirely outside the reach of an EU citizen, they would also have to ensure that any companies they shared personal data or information with also had no possibility of interacting with an EU citizen. Finally, it would likely be extremely costly to exclude European customers from the customer base. Europe is a massive and influential market, and it may be much harder for newer companies to thrive exclusively through domestic customers. Alternatively, the EU has begun to recognize “equivalent” privacy regulatory regimes in other countries, opening up the possibility that companies that operate in these countries can transfer personal data between each other without additional safeguards mandated by the EU. On July 17, 2018, the EU and Japan agreed to recognize each other’s data protection systems as equivalent, creating the “world’s largest area of free flow of data.” 18

Even if a company could theoretically avoid the ambit of the GDPR, states such as California have already begun to enact reactive legislation in response to the GDPR as well. The California Senate and Assembly approved the California Consumer Privacy Act (CCPA) on June 27, and it was signed into law by Governor Jerry Brown the same day. 19 In most relevant aspects, the CCPA is similar to the GDPR.


18 Yuki Sako et al., The new EU-Japan personal data deal: EU and Japan to each recognize the other’s personal data protection system as equivalent – What it means for business and next steps, LEXOLOGY (Aug. 27, 2018), https://www.lexology.com/library/detail.aspx?g=b867c06e-3067-4192-b5fb-7818a067900f [https://perma.cc/YW8M-K8JJ].

19 See Kexin LaCroix, Privacy Rights, Liability Exposures, and Potential D&O Claims, THE D&O DIARY (2018),
Experts predict that the United States Congress will also soon enact their own privacy legislation, creating preemptive federal legislation that will reach any US-based company, whether or not they are subject to the GDPR.

On a more specific level, the GDPR is applicable to individuals, organizations, and companies that are either ‘controllers’ or ‘processors’ of personal data. The GDPR imposes the highest level of responsibility and liability on controllers of information. A “controller” (applicable to the analysis in Chapter IV) is an entity that “determines the purposes and means of the processing of personal data.” Controllers are fundamentally companies that collect data from users themselves. Controllers have strict obligations to communicate with data subjects regarding the processing of their personal data, and their rights in relation to that processing, “in a concise, transparent, intelligible and easily accessible form, using clear and plain language.” However, there is an increased level of liability associated with the responsibility of controllers to choose processors that provide sufficient guarantees to implement appropriate technical and organizational measures that are compliant with the regulation. Therefore, there is an associated watchdog responsibility placed on controllers over their processors. This means that when companies share the data they collect with other companies, they are required to be certain that the processor (and anyone else the processor shares data with) is fully compliant with the GDPR, or else the controller could be vicariously in violation of the

https://www.dandodiary.com/2018/10/articles/uncategorized/privacy-rights-liability-exposures-potential-claims/ [https://perma.cc/24HV-L7AR]. Although the CCPA is similar in many aspects to the GDPR, there are certain significant differences. The CCPA extends to the personal information of “households” rather than just consumers, provides the right to a deletion request for any reason (whereas the GDPR establishes six triggers of the right), and has an absolute right of data portability. Cal. Civ. Code §1798.100, 105, 140 (2010).

20 Regulation 2016/679, supra note 1, at 3-4.

21 This paper will mainly explore the obligations of controllers of information because most, if not all, roboadvisors will qualify as a controller since they personally collect the information from the user.

22 Regulations 2016/679, supra note 1, at 33.


24 Regulation 2016/679, supra note 1, at 16.
GDPR and subject to the same fines that would be imposed if they had committed the direct offense.

Moreover, the definition of personal and sensitive data under the GDRP is very broad when compared with other privacy regulations. Personal data is defined by the GDPR as “any information relating to an identified or identifiable natural person ... who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”25 So, online identifiers like IP addresses and cookies could qualify as personal data since they can be linked back to an identifiable person, depending on how strictly the regulators consider the “personal data” definition.26 Something as insignificant as the answer to a password protection question like “what is your mother’s maiden name?” technically qualifies as personally identifiable information and could fall within the jurisdiction of the regulation.

The Information Commissioner’s Office (“ICO”), the original drafter of the regulation, will be responsible for ensuring enforcement of the GDPR. The regulation’s enforcement is creating the biggest cause for concern in the privacy community and corporations alike as the ICO has the power to impose massive fines on any business that does not comply with the GDPR. The current minimum fine is €10 million or 2% of annual turnover per offense, while the ICO has the authority and discretion to impose fines as high as €20 million or 4% of annual turnover (whichever is higher) for more substantial offenses.27 Any violation of the GDPR is subject to a sanction by the ICO; there is no violation too small—which caused many corporations to panic about how to successfully overhaul their existing privacy system to avoid financial penalty by the implementation date in early 2018.28 Additionally, a shareholder suit has already arisen against

25 Regulation 2016/679, supra note 1, at 33.
26 There is no distinction between personal data when it is collected about people in private, public, or work roles.
27 Regulation 2016/679, supra note, at 83.
Facebook alleging that the company’s most significant recent stock price drop was linked to a misrepresentation regarding compliance with the GDPR. The fact that a suit arose so quickly suggests that even if a company does not face ICO fines, they nonetheless will remain vulnerable to costly shareholder litigation.

III. What is Robo-advising?

Automated advisors, commonly termed “roboadvisors,” have begun to gain traction in the financial services market due to the increased popularity of low-cost automated investment options. Broadly, “in the popular press, a ‘robo advisor’ is an automated investment service, most likely based in San Francisco, which competes with financial advisors by claiming to offer equally good, if not better, financial advice and service at a lower price.” Roboadvisors provide customers with the opportunity to create a portfolio based on their individual characteristics and preferences. Instead of having to pay for a wealth management advisor, people can use the algorithms on the platform to receive customized investment recommendations. Therefore, roboadvisors allow more people, who would typically manage their investments independently, to have access to affordable investment and financial advice. The attractiveness of a roboadvisor is that it will provide better returns to users than them trying to manage their investments independently in the absence of having any kind of oversight.

Importantly, roboadvisors are nearly completely automated, requiring a very minimal number of employees to function. Therefore, the appeal of this business model is that “the money saved not paying a human is passed through to the customer, resulting in younger, less affluent, less investing-savvy folks being able to get in the game.” Indeed, it seems that this prediction is becoming a reality. Assets smaller players out of the market either by bankrupting them or imposing such a financial burden that the company cannot pay to remedy the harm and pay for changes to ensure it does not happen again.

30 Baker, supra note 2 at 719-20.
under management by roboadvisors are projected to grow 68% to $2.2 trillion by 2022. Startups and existing players alike are recognizing the demand. In addition to startups like Betterment and Acorns, “Charles Schwab and Vanguard are now using robos to supplement their full-service offerings.” Popular roboadvisors for 2017 include Betterment, Personal Capital, Schwab Intelligent Portfolios, SigFig, and Wealthfront.

Roboadvisors work by collecting a series of voluntarily provided data points from users. These could include, age, sex, dependents, income, risk tolerance, goals, upcoming expenses, and health history to create a personalized portfolio. Roboadvisors then put these data points into algorithms to build a diversified portfolio and update it regularly as the market or the consumers’ needs change. Typically, roboadvisors charge a small service fee, but are much cheaper than wealth management advisors because there is minimal human interaction. Users trust the algorithms to make recommendations, and typically do not have any discussion with a human before making investments. Fees typically range between $15 to $200 per month, with a 0.15%-0.5% asset fee per year. However, for investors that want a human dimension to their investing, roboadvisors often charge a higher fee for a “hybrid” roboadvising system, whereby people can talk to someone on the phone regarding their investments.

IV. THE IMPACT OF THE PROVISIONS OF THE GDPR ON ROBOADVISORS

A. General Overview

Robo-advisors are controllers of information, designed on the basis of collecting personal data from consumers to make a logical and
personalized investment portfolio based on specified algorithms. Therefore, roboadvisors are collecting PII as controllers according to the GDPR. Moreover, privacy experts suspect that every “website that drops tracking cookies or apps that retrieve usage information [will be] subject to the GDPR.” Assuming that roboadvisors have an online presence and can reach European customers, roboadvisors are then subject to the GDPR. While the “riches to be won by disrupting the financial services industry provide more than enough incentive to rush [roboadvising] technology to market,” this could be too costly a strategy to pursue in light of the financial penalties imposed by the GDPR.

When a consumer chooses to invest through a roboadvisor, they typically are required to provide basic information such as their name, address, date of birth, contact information, payment details, and tax information, in addition to more unique information regarding goals and risk tolerances. Likewise, in the home mortgage sector, helping consumers get the best mortgage rate requires taking the “consumers’ financial situation into account, including likely household income over time, amount and timing of household financial obligations, risk factors associated with the kind of mortgage in question, the likely length of time before sale of the home, [and] the consumers’ credit rating.” Since the roboadvisor is the one collecting the information, they are a data controller, held to the highest standards by the GDPR. In addition to the roboadvisor, their contractual agents that process the information must all be compliant with the GDPR or else the roboadvisor could be held liable as well. Examples of applicable processors include a transfer agent that will use the information to update the shareholder register of the fund. Also, any investment managers that the roboadvising company does employ will also need to be compliant when they are profiling investors to identify new investment opportunities.

Compounded on top of regular GDPR requirements, roboadvisors would be considered high-risk controllers, rather than a risk or low-

---


37 Baker, supra note 2, at 2.

38 Baker, supra note 2, at 9.
risk controller, as defined by the regulation.\textsuperscript{39} As a high-risk controller, roboadvisors are required to conduct Data Protection Impact Assessments (“PIA”) and consult with a Data Privacy Authority (“DPA”) prior to processing information that involves the “systematic and extensive evaluation of [PII], which is based on automated processing. . . on a large scale. . . in particular using new technologies.”\textsuperscript{40} Roboadvisors fit cleanly under this definition. First, they are profiling individuals based on their unique qualities to determine suitable investments. The profiling requires the aggregation of various data points of personal sensitive information. Moreover, roboadvisors’ appeal is that they are making investment recommendations through the innovative use of technological solutions. Roboadvisors engage with PII on a regular and systematic basis by continually re-processing personal data as market conditions change to ensure that investments are still advantageous based on the customer’s financial situation and goals. Therefore, roboadvisors particularly need to be certain that they are responsibly handling sensitive data according to the provisions of the GDPR and will likely need to have a PIA done by a law firm to be compliant with the GDPR. The PIA will require “(1) a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller, (2) an assessment of the necessity and proportionality of the processing in relation to the purpose, (3) an assessment of the risks to individuals, and (4) the measures in place to address risk.”\textsuperscript{41}

The DPA must also be an integral part of the corporation at every level, ensuring compliance with the privacy regulation. France has even gone so far as to recommend that all businesses that process EU personal data should appoint DPAs, regardless of the systemic monitoring’s scale.\textsuperscript{42} Startups with a limited early-stage budget will,

\textsuperscript{39} Regulation 2016/679, \textit{supra} note 1 at 53.

\textsuperscript{40} Regulation 2016/679, \textit{supra} note 1 at 53-55.


therefore, have to hire a data privacy expert when they start interacting with customers. Although roboadvisors keep costs low by having a small employee base and often require consumers to pay extra to have a human interaction component, roboadvisors will not be allowed to make consumers pay to speak to a human if the consumer wants to invoke one of their GDPR rights. Likely, since roboadvisor companies will need to hire a DPA anyway, in addition to ensuring compliance structures are in place, this person can be responsible for handling consumer privacy reports and cases for their respective roboadvisor. Roboadvisors will just need to ensure that there is a large enough staff to respond without undue delay to customer requests. A single DPA will likely not be sufficient if there is an event like a data breach with hundreds of consumers requesting information about their data at once.

The GDPR is going to have a disproportionate impact on startups because they typically do not have an existing privacy protocol in place at the early stages of the company. There are few people that are privacy professionals, so contracting someone to review and implement privacy policies can be costly when funding is minimal. However, startups and large corporations alike are subject to the GDPR, so startups will have to ensure compliance with the regulation or otherwise risk being bankrupted by the hefty fines imposed by the ICO. Notably for startups, privacy experts concede that the GDPR is too massive to implement all at once. In a study by McKinsey, most of the companies they surveyed, regardless of their size, stated that they would not be fully compliant by the GDPR’s implementation date. Therefore, it could be advantageous for startups with a smaller budget to wait and see what the ICO chooses to focus on. Likely, the ICO will first go after large corporations with assets, such as Facebook and Google, to set the stage for the seriousness of the GDPR. However, if roboadvisor startups do not do anything to start working toward the GDPR, they likely will have a very small timeframe to ensure compliance before they are the target of ICO regulatory enforcement. Additionally, there is no promise that the ICO will first target big players, so roboadvisor startups should be proactive with compliance. Unfortunately, corporations will be forced to pass the cost of GDPR compliance to the consumer, potentially detracting from the

competitive edge that roboadvisors have by being low-cost alternatives to larger financial institutions. Moreover, potential D&O insurance coverage for breaches is uncertain, further enhancing the potentially deleterious effects of the GDPR on the entrepreneurial landscape.

Finally, increases in sanctions have already demonstrated a substantial influence on de-risking in the banking industry. It is concerning to consider that high fines may change the risk-reward perception of companies—leading to a financial incentive to exit riskier areas of business instead of taking on the additional costs necessary to comply with the regulations. Applied to roboadvisors, the companies leading the way in the industry are inherently very high risk in order to facilitate innovation. The possibility of steep sanctions by the ICO may be too much for these companies to bear at such an early stage of the business life-cycle. Roboadvisor companies will be forced to either wait and hope that the ICO goes after large corporations first, or somehow find a way to budget for the personnel and technology necessary to ensure that the company can comply with the GDPR while remaining competitive with low prices or end the service.

In order to preserve the normative goals of enhancing and standardizing the privacy regulatory landscape while also avoiding disproportionately dampening entrepreneurial growth, it could be suitable to have the ICO adopt exceptions and modifications for emerging growth companies, similar to the United States’ Jumpstart Our Business Startups (JOBS) Act. The regulation is likely to be prohibitively expensive for many startups to fully comply with and equally costly to defend in the case of a breach. The ICO, therefore, could instead trigger the full applicability of the GDPR when a company passes a certain threshold, such as number of users or annual gross revenue. This would indicate that the company has reached a sufficient level of sophistication to be expected to be fully compliant with the GDPR. Smaller and newer companies, on the other hand, could be required to comply only with the more essential consumer-protection elements of the GDPR. Rather than forcing them to stretch an already limited budget across a massive regulation, and haphazardly doing their best to comply, this may allow emerging companies to first establish a strong privacy-minded foundation while they are afforded the opportunity to take risks and grow. While there

are currently no indications that the ICO has considered such a system, it would be prudent to better attempt to achieve privacy goals with a mind toward the unique challenges that face emerging companies.

B. The Right to Be Informed

The past year has unfortunately seen an unprecedented number and frequency of ransomware and other cyber-attacks. To combat this vulnerability, the GDPR instituted the right to be informed. An integral component of this right is that controllers and processors must report any “destruction, loss, alteration, unauthorized disclosure of, or access to people’s data.”

Depending on the severity of the situation, determined by what and how much data was compromised, the reporting may either be to the country’s data protection regulator or the person whose data was impacted. For severe violations, the GDPR imposes a notification requirement to impacted parties “without undue delay.” Unless the breach is unlikely to result in any risk for individuals, every breach, regardless of the severity, requires a mandatory breach notification to a supervisory authority within 72 hours. For an early-stage roboadvisor without the capital to institute an expansive security system (making them a more likely candidate for a breach) and without a history of credibility to back them up, the breach reporting requirement could be terminal. This also means that roboadvisor companies must have a cyber incident response plan in place before a breach occurs because it will likely take more than 72 hours to design one and respond if a plan is not in place when a breach happens. Information processors that are contracted with the roboadvisor will also be required to report any breaches to the controller/roboadvisor without “undue delay.” Since roboadvisors have so much personal information regarding a consumer’s assets and personal characteristics, roboadvisors should expect to be more likely targets of breaches and should be prepared to notify consumers within 72 hours when one occurs.

Moreover, the right to be informed includes being informed about how information is processed. The GDPR requires that roboadvisors

---

45 Regulation 2016/679, supra note 1, at 34.

46 Regulation 2016/679, supra note 1, at 52-53.

47 Regulation 2016/679, supra note 1, at 52.
inform the investor about the legal basis for processing their information.\textsuperscript{48} This information should be readily accessible and in a clear and concise form. Individuals maintain a right to complain to the ICO if they feel that a roboadvisor is handling their data in a problematic way.\textsuperscript{49} Roboadvisors will, thus, need to be able to provide consumers with clear answers as to why they are collecting every piece of data and how it is relevant to the underlying recommendations being made or the functionality of the roboadvisor. Every data point must have an identifiable and explainable purpose understandable by the average EU citizen. As a result, roboadvisors must only collect information that is being used for a purpose—part of the GDPR’s data minimization aspect.

\textbf{C. The Right of Access}

The GDPR covers the lifespan of data. Therefore, even if a customer is no longer using the company’s services, the company is still required to comply with the rights listed under the GDPR, particularly the right of access, as long as they maintain data on the individual. This means that years after a European consumer cancels their account with the roboadvisor, they can request a report from the company that outlines what data the company still retains about the customer and how it has been used (by the controller and processors) during the entire lifetime of the data. To comply with the right of access, McKinsey recommends building a “golden record” of every possible personal-data processing activity that the company engages in—with consumers and employees alike.\textsuperscript{50} This provides an efficient means to respond to massive volumes of requests, reducing costs for roboadvisors. Additionally, roboadvisors can significantly cut their right-of-access costs if they choose to implement a functional non-retention policy for some data points, reducing the amount of data they have to store and report.


\textsuperscript{49} Regulation 2016/679, supra note 1, at 4.

\textsuperscript{50} See Mikkelsen, supra note 44, at 7.
Efficiency and cost-reduction are significant because, relatedly, roboadvisors will not be allowed to charge for complying with a request. This provision is likely to impose high costs on early growth companies with limited capital. Additionally, the GDPR imposes a short time-frame of one month to comply. Roboadvisors will need to have mechanisms in place to deal with a high volume of requests for access, especially in the case of a breach, or else they risk paying fines as discussed in Section II. Roboadvisors can refuse requests that they believe are “manifestly unfounded or excessive,” but if they do this, they still must inform the customer of their grounds for refusal and let them know that they have the right to complain to a supervisory authority.\(^{51}\) If the complaint is successful, this can lead to a judicial remedy, imposing more costs on the company. This process must also be done within a month.\(^{52}\)

D. The Right of Rectification

The right of rectification establishes that a consumer has the right to correct any information that a data controller or processor uses. Therefore, a roboadvisor must comply with any request by a customer, free of charge and without undue delay, to change their data. Typically, a roboadvisor has one month to reply.\(^{53}\) This can obviously impose great costs. However, unlike other GDPR provisions, data rectification is likely already in the best interest of the roboadvisor. Roboadvisors have an existing incentive to keep the information accurate and up-to-date since the algorithms are dependent on correct information to make tailored decisions and recommendations.

Many roboadvisors already require that customers log in according to a set timeframe and review their provided data as well as update the company of any changes. Therefore, there is not much that roboadvisors will additionally need to do to comply with the GDPR’s right to rectification. The biggest change will be ensuring that there are systems in place to quickly respond to requests and guaranteeing that all requests are indeed complied with and changed according to customer wishes. This can be difficult to do when there are many

\(^{51}\) Regulation 2016/679, supra note 1, at 40.

\(^{52}\) Regulation 2016/679, supra note 1, at 40.

\(^{53}\) Regulation 2016/679, supra note 1, at 40 (This can be extended by two months where the request for rectification is complex.).
requests in a short period of time, so roboadvisors must ensure that they are organized regarding processing and responding to requests. Roboadvisors may find it easiest to list all data that has been collected on a consumer on their login page, and allow them to update the information, rather than having them contact a company employee to effect the change.

E. The Right of Erasure

The right of erasure establishes that customers have a “right to be forgotten.” The right of erasure essentially means that if data is (1) no longer necessary for the purposes collected, (2) the data subject withdraws consent, or (3) the data subject objects to data processing, then the roboadvisor must completely destroy all personal data without undue delay. Just like the right of rectification, a consumer has the right to require the roboadvisor to destroy any data that they maintain that is not absolutely necessary for the functioning of the roboadvisor or that the data subject does not want the roboadvisor to take into account when making investment decisions. This provision could compromise the ability of roboadvisors to provide the best possible recommendations—when they have less information about the consumer, they have a narrower picture of what risks and goals they must account for. This could, in turn, hurt the overall success of the roboadvisor because they will have less data to analyze on all their consumers (especially in relation to existing corporate giants employing roboadvising technology), and they may have more difficulty providing competitive returns. If roboadvisors cannot consistently show higher returns than an independently managed fund, it is likely that they will lose a huge consumer base and will not be able to compete in the market. Moreover, if data are stored in various locations, the roboadvisor will be liable for ensuring that data are entirely erased from every system they have. However, roboadvisors can likely concede that consumers should have the right to have investments made only on the information they want taken into account, so the right of erasure will not pose severe threats as severe to roboadvisors as they have to search engines.

54 Regulation 2016/679, supra note 1, at 43.
F. The Right to Restrict Processing and the Right to Object

Consent is a massive requirement of the GDPR under the right to restrict or object to use of personal data. While the United States is primarily based on an “opt-out” consent system, where companies can use data until a consumer requests that they no longer use it, the GDPR requires that all use of personal data be “opt-in,” where consumers will have to assent to give the company the right to use their data.\(^{55}\) Moreover, consent cannot be inferred from silence, pre-ticked boxes or inactivity.\(^{56}\) Therefore, consumers entirely control when and how their information is used. It will be extremely administratively burdensome to ensure that the consumer has explicitly consented to every use of their data. Moreover, consumers can withdraw their consent at any time.\(^{57}\) This means that an investment roboadvisor will have to adjust the consumer’s entire portfolio by re-running the authorized data through the algorithm. For non-investment roboadvisors, there may be concerns if the algorithm recommends a different mortgage or insurance provider and the consumer cannot easily change their existing provider.

G. The Right to Data Portability

The right to data portability is the “right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.”\(^{58}\) It is a new regulatory concept that shares no ancestry with the previous Data Privacy Agreement. The information must be provided in a commonly used and machine-readable format, so that the new controller can easily import and make use of the data.\(^{59}\) Importantly for roboadvisors, consumers may request that data are sent to a competitor. On its face, this means that competitors could theoretically analyze the roboadvisor’s data points and investment recommendations to improve their own processing.

---

\(^{55}\) Regulation 2016/679, supra note 1, at 37.

\(^{56}\) Regulation 2016/679, supra note 1, at 6.

\(^{57}\) Regulation 2016/679, supra note 1, at 8.

\(^{58}\) Regulation 2016/679, supra note 1, at 45.

\(^{59}\) Regulation 2016/679, supra note 1, at 13.
techniques according to the roboadvisor’s model and make their returns marginally better. In such a small niche market, this possibility is concerning. This fear is irrational, though, because the GDPR says that the only information that must be portable is what the consumer has “provided to” a data controller. 60 Experts suggest that this limitation then “excludes any data which has been derived from the original data.” 61 Therefore, the information sent to a competitor would probably only involve the basic registration questions, likely similar across platforms and easily discoverable by competitors.

V. CONCLUSION

The GDPR is certain to require companies, and roboadvisors in particular, to devote significant financial resources and time to avoid steep sanctions by the ICO. While the right to rectification will require fewer changes for compliance, other rights, such as the right to portability, may prove problematic for roboadvisors, since such new rights require an overhaul of most existing privacy policies and procedures. Companies will likely be forced to prioritize which provisions to tackle first and then adjust as the ICO initiates enforcement. Many fear that the heavy costs that sanctions and compliance impose will push startups out of the market. It is also not yet clear whether traditional D&O insurance will apply to breaches, enhancing the risk for already fragile entrepreneurial companies. 62 However, if roboadvisors can manage to comply with the monstrous GDPR, they will likely find it a much simpler task to effectively compete with existing large players in the financial industry.

60 Regulation 2016/679, supra note 1, at 45.


62 See LaCroix, supra note 20.