[[1]](#footnote-1)

**Emerging Impact of General Data Protection Regulation on the Financial Industry**

Trisia Baltazar, Turner Barnett, Adrian Boone, Chad Daily, Mate Kovacs, Joseph Morrison

*Abstract*— The GDPR (General Data Protection Regulation) has been in effect for almost five months, and it has already made a significant impact on the day-to-day operations of any businesses that operate in the digital sphere. It is one of the strongest, if not the single strongest data protection law in the world and comes with the full backing of the European Union, who have proven themselves very willing to exercise their right to enforce it when necessary. The GDPR will likely serve as the basis of national data privacy laws going forward, even if it is itself not adopted at a global scale. As such, organizations – particularly those operating within the financial sector – will need to be aware of the impacts that the GDPR can have on the way that they do business, as well as the ways in which their compliance with the GDPR can be leveraged as a business advantage, as consumers become more savvy and more concerned with a company’s policies regarding data privacy. This paper will review the impact that the GDPR has had and will continue to have on financial institutions and will suggest approaches to compliance and leverage.

*Index Terms*—

# INTRODUCTION

The General Data Protection Regulation has impacted many businesses worldwide. The General Data Protection Regulation was implemented in May 2018 in the European Union. The regulations were put in place to protect personal data and provide transparency across organizations who collect personal data from individuals. The financial industry is one of many sectors that have been greatly impacted by these regulations because a significant amount of the companies operates globally, including in the EU. These organizations include banks, money transfer companies, and ecommerce retail giants who service millions of people. The impact of these regulations can be both financial and reputational if the organizations are not in compliance. Although there are many risks not complying with these regulations, companies can leverage their compliance to have a competitive advantage, especially in the financial sector of the market. More importantly, it gives the individual customer more insight into what their data will be used for and provides them with straightforward interpretations of the use of their data.

# Money Transfer companies

PayPal and Google Pay are both American companies that operate worldwide. They are money transfer companies that help big and small businesses get payment from customers. GDPR is impacting major financial institutions in different ways, PayPal and Google Pay is just one of them. These companies play a huge role in the payment app industry is Google. Google has an app called “Google Pay” which allows users to send money from bank accounts to any email address. Not only that, but it also allows users to make purchases online or at brick and mortar stores that accept it as a form of payment. PayPal is very similar to Google Pay. PayPal acts as a money transfer site as well as serves as an electronic alternative to cash and checks. Because of their global reach, Google Pay and PayPal are required to abide by GDPR’s new regulations regarding personal data.

## Impact of GDPR

Both companies are not taking a major toll from GDPR. In fact, both are still well in the business and only a couple tasks were done to become GDPR compliant. PayPal has established a Global Privacy Program and Framework and a team dedicated to ensuring that PayPal is GDPR compliant. They have updated their User Agreement and Privacy Policy, as well as their internal policies and procedures. Both Google Pay and PayPal are continuing to stay up to date with the policies to come as well as letting EU customers get more control for their personal data as well as opt-outs. Google Pay is only one of the many branches that Google must make GDPR compliant. They must keep applications such as the search engine, Gmail and all their advertising and measurement services up to date. So far, they have been GDPR compliant and as a money transfer company that depends on partnerships with other businesses, it is important to stay up to date with policies to keep business with them.

## Ensuring Compliance

PayPal is an American company that operate worldwide with online payments, which means they are one of the many companies that must comply with GDPR standards. Many companies operating with Europe or located in Europe must sign an agreement to stay on business with PayPal and vice versa. There are virtual agreements such as “PayPal Website Payments Pro and Virtual Terminal Agreement” that were requested by many businesses for PayPal to release [1]. This agreement is an example of Data Processing Agreement which ensures that PayPal is compliant with GDPR, thus requesting that the businesses they work with are also GDPR compliant [2][3]. PayPal is both a Data Processor and a Data Controller:

“The Data Controller, alone or jointly with others, determines the purposes and means of the processing of personal data, while the Data Processor is processing data on behalf of the Data Controller…Both the Data Controller and Data Processor have an obligation to protect personal data according to the GDPR. For Data Processors, those obligations should be clearly determined by the various parties with data protection terms in their agreements to make sure that customers’ personal data is lawfully processed. [4]”

The Data Processor and Data Controller have different roles, so it is important for PayPal and other money transfer companies to set up different agreements and policies that will encompass both roles.

Google is also very openly complying with GDPR’s rules and regulations. On their site, they list several changes they’ve made to be GDPR compliant. These go as follows [5]:

1. “Committing in our contracts to comply with the GDPR in relation to our processing of customer personal data in all Google Cloud Platform and G Suite services
2. Offering additional security features that may help you to better protect the personal data that is most sensitive
3. Giving you the documentation and resources to assist you in your privacy assessment of our services
4. Continuing to evolve our capabilities as the regulatory landscape changes.”

Google must continue to offer these services to operate within Europe and show that they remain GDPR compliant.

## Competitive Advantage by GDPR

PayPal may lose some partnerships with businesses that do not comply with GDPR, but a lot of their partners are also active in Europe, so by complying with GDPR, they will strengthen bonds with those businesses as well as maintain its big name as a money transfer company. Google can leverage this into a competitive advantage against other companies in several ways. For one, they can promote their GDPR compliance to their customers. Currently, Google has numerous pages of information available about how it is complying with GDPR [6]. Everything from their updated terms and conditions to how they will be transparent with user data [14]. By doing this, Google can gain a competitive advantage over another company that might not be so transparent as customers will want to have more control over their data. Another way Google can use GDPR to gain a competitive advantage is by being proactive. By achieving GDPR compliance before others, consumers will more likely pick Google over a non-GDPR compliant organization. This includes normal customers, as well as other businesses who won’t want to risk non-compliance by dealing with other non-compliers. Overall, Google and PayPal are making sure that all their products are GDPR compliant and are gaining a competitive edge while doing so.

# Banks with online aspects

## With the introduction of the GDPR, the role of banks as custodians of customer data has shifted. Where it was once enough to simply be secure in their collection and storage of information, the GDPR has brought a new focus on transparency as a core value that must be ensured. Considering the weight and impact that GDPR violations can have on a business, it’s critical that financial institutions take every necessary step to ensure their compliance with this new legislation.

## Banks must be able to adjust to the new and enhanced consent requirements; mechanisms must be in place to secure and safely store customer content. This mechanism must be able to adapt to changes in consent settings and efficiently manage customer preferences.

## In addition, institutions must define a clear policy on data portability, to properly account for instances when customers request to have their data ported from one organization to another — when switching banks, for example, or when transferring an account from one branch to a different branch within the same business.

## Existing procedures for data retention and erasure must be upgraded or supplanted with enhanced versions that are capable of handling the new rights of customers in terms of access, correction, erasure, etc. These procedures must also enable the tracking and deletion of data when requested by customers.

## Bank of America and HSBC are two of the largest banks in the world. Bank of America operates out of Charlotte, NC while HSBC operates out of London [11]. Bank of America currently holds 2.28 trillion in assets and HSBC holds 2.52 trillion [12]. The functions of these banks range anywhere from commercial banking and transaction services, to credit lending and investment banking as well as online banking functions. Although the headquarters of these banks are not located in the European Union, they are impacted heavily by the GDPR because of their operations in the countries within the EU. Equations

## Impact of GDPR

The data collected on the customers of these banks have been the focal point of the new GDPR law passed in May of 2018. Several areas of these banks have been impacted by the implementation of the GDPR, including Client Management, Trade Lifecycle, and Support Functions [13].

The impact of the GDPR of major financial institutions, especially banks, that operate in the EU have been considerable. Since the companies acquire sensitive data regarding their customers, several requirements were established to protect these individuals. Financial risks for not complying with GDPR can be damaging to the bank if not followed properly. Most importantly, the reputation of these companies can suffer severe and detrimental consequences by not complying to GDPR standards.

With GDPR being very robust and intense, customers expect companies to protect their personal data by implementing more powerful technologies and processes to ensure their information is safe and secure. Customer data can no longer be used as these banks see fit. GDPR gives customers better ground to stand on and puts pressure on banks to be more transparent and make it clear what is being shared and protected in a seamless and easy to understand way. This leads banks and other financial entities to abide by certain compliance regulations, which are lengthy and play an important role in business strategy moving forward.

## Ensuring Compliance

GDPR compliance starts from the top-down. The goals of executives and stakeholders must align; the multi-disciplinary nature of GDPR compliance programs means that anything less than complete alignment will result in slowdown and difficulty. Organizations must likewise appoint a Chief Data Officer (CDO) to serve as needed representation in the C-suite. The CDO can then work with the organization’s in-house legal team to determine the best approach: business-oriented, system-oriented, or a combination of both.

Research from International Data Corporation [10] shows that there is nearly an even split between companies that see GDPR as an unrealized opportunity, and those that see it as an unwanted obstacle. In less regulated industries such as manufacturing, this split is even more pronounced; 80% of organizations within the manufacturing sector consider the GDPR to be an obstacle, because of their comparably lesser experience in matters of data regulation and legal compliance.

The only thing that keeps compliance from being a benefit of its own is perspective. By displaying competency and control over their data, an organization can invite business from other organizations who seek said competency when looking for partners and deals. The penalties that result from failure to adhere to the standards set by the GDPR are so harsh that no one will be willing to put themselves at risk of even third-party non-compliance.

## Competitive Advantage by GDPR

Furthermore, the restructuring that will be required in pursuit of GDPR compliance will allow companies to assert more granular control over their data, which is easily one of the most valuable assets that any organization can possess. Being able to take a more accurate look at their data, and in the process determine what is truly important and what’s simply occupying much-needed space, will allow companies to leverage that data more effectively and efficiently, in addition to providing a future basis for data restructuring and data governance in a fashion that is more consistent with the best practices of the organization’s industry.

# Online Stores/E-Commerce

With the introduction of the General Data Protection Regulation (GDPR) on May 25, 2018, all online stores and businesses are required to abide by the rules set in place if the goods and services that they provide are available to people in Europe. GDPR regulations apply to all online businesses regardless of location given that European citizen personal data is used in accessing their goods and services. Major online electronic commerce organizations such as Amazon, Shopify, and eBay have been affected by the introduction of the General Data Protection Regulation, as they deal with the personal data of online customers in Europe and around the world.

## Impact of GDPR

The General Data Protection Regulation (GDPR) had significant impacts on the world of e-commerce. Many e-commerce websites not only had to figure out they themselves would remain compliant, but they needed to come up with a plan to make sure that people using their website to sell things could also remain compliant. For example, Amazon not only needs to make sure that they remain compliant with GDPR regarding their web hosting services, advertising services, and so one but they also need to make sure that any third-party seller using their website that is selling within the EU needs to remain compliant with GDPR. This is quite a challenge because they need to spend time and resources to make sure their own activities and the activities of third parties selling through their website are compliant. This means they are going to need to spend extra time and money compared to other industries that only need to worry about themselves being compliant.

## Ensuring Compliance

To ensure compliance with the General Data Protection Regulation (GDPR) regulations, online stores that interact with European customers are forced to change the way that customer personal information is collected and handled. Many online stores, Shopify for example, have updated their Terms of Service regarding how they process European customers’ personal data, and they have also updated their Privacy Policy and Cookie Policy to ensure that the information that they collect is in line with the regulations brought in by the GDPR. Shopify has also implemented a feature under the customer’s profile that can be utilized to review the personal information that Shopify has access to, as well as a feature to remove all personal information that Shopify has of the customer [8].

For eBay to ensure compliance with the GDPR, they have also updated their User Privacy Notice to reflect the changes that the GDPR has brought. eBay has made the customers personal data easier to access and explain in more detail what they use personal data for. Prior to the GDPR being enforced, eBay did not have a feature on their online website to allow users from the European Union to modify or delete their personal information. After the GDPR was introduced, eBay updated their site to abide by the laws put in place by the GDPR so that European Union customers were given the right to modify, update, or delete the personal information that eBay had gathered [7].

## Competitive Advantage by GDPR

A major competitive advantage that e-commerce sites such as eBay stood to gain during the introduction of the GDPR was through the creation of their tutorial on how to remain GDPR compliant. What this means is that sites like eBay created tutorials that gave easy step by step instruction to their users on how they could remain compliant with the GDPR and continue to sell items in the EU. When GDPR was announced, for e-commerce sites it was a race to see who could either put out the first tutorial or who could make their tutorial the easiest to use. If I was a seller willing to use whatever e-commerce site, I would be swayed into using whichever made it the easiest for me to comply with the GDPR rules. This drive to have a competitive advantage led e-commerce sites to spending a great deal of time and money to make it as easy as possible for their users to continue to use their site while remaining compliant with GDPR.

# Conclusion

Personal data is the focus of the General Data Protection Regulation. As globalization has become a norm, many companies outside the EU and EEA are affected by this policy. Online transactions have also become very popular throughout the years. Banks, money transfer companies and e-commerce companies have all handled GDPR in a similar way. From updating their privacy policies to creating new teams and roles to ensure compliance with GDPR and upcoming policies, it has become a fact that staying GDPR compliant will give companies a competitive edge while to some, compliance ensures that the business will stay alive. As organizations become more GDPR compliant, consumers and clients are now being informed on how sensitive data is being handled as emails of policy changes raced throughout the web. Knowledge of how the data is being handled has become more transparent and it is up to these organizations to maintain and comply to the transparency.

References

[1] PayPal Website Payments Pro and Virtual Terminal Agreement. September 11, 2018. Available: <https://www.paypal.com/uk/webapps/mpp/ua/provt-full?locale.x=en_GB>

[2] PayPal Stories Staff. GDPR for smaller organisations. April 20, 2018. Available: <https://www.paypal.com/stories/uk/gdpr-for-smaller-organisations>

[3] Information Commissioner’s Office. Getting ready for the new UK data protection law. 2018. Available: <https://ico.org.uk/media/for-organisations/documents/2258293/eight-practical-steps-for-micro-business-owners.pdf>

[4] PayPal Website Payments Pro and Virtual Terminal Agreement. September 11, 2018. Available: <https://www.paypal.com/uk/webapps/mpp/ua/provt-full?locale.x=en_GB>

[5] Google. Google Cloud & the General Data Protection Regulation (GDPR). 2018. Available: <https://cloud.google.com/security/gdpr/>

[6] Google. Businesses and Data Compliance Page. 2018. Available: <https://privacy.google.com/businesses/compliance/#?modal_active=none>

[7] eBay. Your GDPR obligations when selling on eBay. 2018. Available: <https://www.ebay.com/help/selling/selling/gdpr-obligations-selling-ebay?id=4768>

[8] Shopify. General Data Protection Regulation (GDPR). 2018. Available: <https://help.shopify.com/en/manual/your-account/GDPR>

[9] Amazon. General Data Protection Regulation (GDPR) Center. 2018. Available: <https://aws.amazon.com/compliance/gdpr-center/>

[10] B. Duncan, Ready or Not? GDPR Maturity Across Vertical Industries, 2017. Available: <https://us.blackberry.com/content/dam/blackberry-com/PDF/enterprise/wp-gdpr-maturity.pdf>

[11] HSBC. About HSBC. 2018. Available: <https://www.about.hsbc.co.uk/>

[12] Bank of America. About Us. 2018. Available: <https://www.bofaml.com/en-us/content/about-us.html>

[13] R. Cryer, C. Dicusar, N. Snyder, A. Lawson. General Data Protection Regulation (GDPR) Are You Prepared? 2017. Available: <https://www.brickendon.com/wp-content/uploads/2017/09/Brickendon-Consulting-Insight-GDPR-are-you-prepared-digital-UK.pdf>

[14] W. Malcolm. Google. Getting ready for Europe’s new data protection rules. Aug 8, 2017. Available: <https://www.blog.google/around-the-globe/google-europe/gdpr-europe-data-protection-rules/>

1. [↑](#footnote-ref-1)