ACAMS® | Advancing Financial Crime Professionals Worldwide

The Importance of Incorporating Data Privacy into Anti-Money Laundering and Anti-Corruption Compliance Programs

Jessica R. Hughes, Esq., CAMS

Introduction

Companies in the U.S. have a number of compliance obligations with which they must comply when it comes to conducting business internationally. Anti-money laundering (AML) and anti-corruption regulations, which require a company to conduct due diligence on those entities and individuals they intend to do business with, can create a need to consider the impact of international data privacy regulations.

Failing to treat data privacy compliance with the same duty of care as other compliance obligations can result in fines and reputational damage. Some countries' privacy laws criminalize violations and levy individual liability and jail time. Data privacy laws vary by country and can be comprehensive and complex. The only way a company can avoid such liability is to carefully review and analyze a country's data privacy law as it applies to its due diligence processes.

While this paper will focus primarily on the conflict between U.S. AML and anti-corruption statutes and their due diligence and know your customer (KYC) requirements and the relevant restrictions imposed by the EU's General Data Protection Regulation, it is important to carefully consider and analyze the privacy laws of any country wherein business is being conducted.

Due Diligence Obligations

U.S. Anti-Money Laundering Regulations

U.S. AML regulations require that financial institutions within the U.S., and also those with business interests in the U.S., conduct a certain amount of due diligence on their customers.

The Bank Secrecy Act (BSA) imposes requirements, such as recordkeeping and reporting, on financial institutions within the U.S. along with foreign banks with branches and agencies in the U.S.[1] The BSA was amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), which created the customer identification program requirement financial institutions are now subject to.[2] The Financial Crimes Enforcement Network (FinCEN) issues Final Rules, which help clarify what is required of financial institutions when conducting due diligence.

Due diligence is merely one of five components or "pillars" of an effective AML compliance program. The other hallmarks of an effective compliance program, as mandated by FinCEN, are establishing written compliance policies and procedures, the designation of an AML compliance officer, independent audits of the compliance function, and providing compliance training to employees.[3]

[1] (Office of the Comptroller of the Currency, n.d.)
[2] (Office of the Comptroller of the Currency, n.d.)
[3] (Stuart P. Lott, 2016)

FinCEN requires a financial institution to identify and verify individual customers and beneficial owners of legal entities, understand the nature and purpose of the relationship with the customer opening the account, and conduct ongoing monitoring to comply with the "fifth pillar," customer due diligence (CDD).[4] The requirement to identify and verify beneficial ownership interests does not take effect until May 2018. The other requirements are already effective.

The identification and verification of customers component requires a financial institution to collect information and identification from a customer at the time an account is opened. The purpose of collecting such information is for the bank to create a customer profile, which allows the bank to determine the type of activity to expect within a customer's account. Enough information should be gathered to allow the bank to determine what type of activity is commensurate with the occupation or type of business.[5] This includes the types of transactions to and from the account to develop a baseline for transaction monitoring.

Once information has been collected from the customer, a financial institution should seek to verify such information. Information provided by customers at account opening can be verified by obtaining reports from an information reporting agency, country registries, secretary of state registries, conversations with customers and onsite visits to business addresses.

Internet searches and commercial database can also be useful for confirming information provided by customers.[6] Such searches can also uncover politically exposed person (PEP) relationships, or that the customer themselves hold a position of political prominence. Searches of this kind can also reveal whether the customer appears on a sanctions list or watchlist. Negative news searches along with litigation database searches can be done to uncover additional information relating to customers. The same type of due diligence should be done with those individuals with ownership or controlling interest of companies. The financial institution must then make a risk assessment based on the customer's occupation or business operations along with the type of account being utilized.[7]

Customer and beneficial owners should be updated and screened as part of ongoing monitoring. FinCEN has indicated that CDD updates are not expected on a regular basis. Conversely, it is only necessary to update and screen when an event occurs that causes the financial institution to believe that customer information has changed or an event has raised suspicion, such as a transaction not in line with the customer profile.[8]

Financial institutions should employ enhanced due diligence (EDD) procedures when dealing with customers whose profile is classified as high risk. EDD will require gathering more extensive information using open-source searching, commercial databases and putting resources on the ground to conduct an onsite visit.

[4] (Stuart P. Lott, 2016)
[5] (Federal Financial Institutions Examination Council Bank Secrecy Act/ Anti-Money Laundering InfoBase, n.d.)
[6] (Federal Financial Institutions Examination Council Bank Secrecy Act/ Anti-Money Laundering InfoBase, n.d.)
[7] (Federal Financial Institutions Examination Council Bank Secrecy Act/ Anti-Money Laundering InfoBase, n.d.)
[8] (Federal Financial Institutions Examination Council Bank Secrecy Act/ Anti-Money Laundering InfoBase, n.d.)

Customer identification and collecting due diligence as part of a thorough KYC program are just a small piece of a larger AML compliance program.

U.S. Anti-Corruption Regulations

U.S. anti-corruption laws also require U.S. companies conducting business internationally to conduct due diligence on their vendors and third parties. Global companies will also be required to comply with anti-bribery and anti-corruption regulations in other countries wherein they are conducting business.

The Foreign Corrupt Practice Act (FCPA) is a U.S. federal statute which seeks to combat bribery and corruption. The Anti-Bribery Provisions of the FCPA prohibit offers or payments, either monetary or anything of value, intended to influence foreign officials in order to gain improper business advantage.[9] Offers or payments made by third parties on behalf of a company or individual subject to the FCPA are also strictly prohibited.[10] The statute's jurisdictional reach includes companies listed on the U.S. stock exchange, citizens, nationals and residents of the U.S., companies with a principle place of business in the U.S. along with their officers, directors, employees, agents or stockholders acting on their behalf in or out of the U.S.[11] The statute can also apply to non-resident entities or individuals engaging in the statute's proscribed conduct within the U.S.' borders.[12]

The FCPA requires companies, as part of a larger anti-corruption compliance program, to conduct risk-based due diligence on third parties prior to engaging with them, and on an ongoing basis. Due diligence should be conducted on individuals identified by customers along with those identified through company information services. Such searches can uncover PEP relationships. Open-source, negative news searches and litigation database searches should be conducted to be sure the party with which a company intends to engage has not been the subject of prior corruption investigations or other related offenses. Customers and vendors should be screened against sanctions list and watchlists in addition to these searches.

As is the case with AML due diligence, it is recognized that some third-party business partners pose a higher risk than others. Therefore, anti-corruption due diligence is also risk based. Those vendors who pose a higher risk are expected to be more thoroughly screened

[9] (Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, 2012) at 10

[10] (Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, 2012) at 21

[11] (Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, 2012) at 10-11

[12] (Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, 2012) at 10-11

Because of the FCPA's extensive reach, both over the conduct regulated and the parties to which is potentially applies, it is imperative to have a robust compliance program in place especially when dealing with third parties outside of the company.

Data Privacy Restrictions

There are varying degrees of privacy protections offered by different countries. Some countries provide little to no protections, while others provide complex, comprehensive privacy schemes. The type of data being protected, along with the definitions of data type, can also vary among countries. In some countries, data privacy protections are explicitly spelled out by statute. Other countries' data privacy protections are derived from their general constitutional privacy guarantees.

European Union

The countries of the EU have likened the protection of personal data with other enumerated fundamental rights, such as the right to life and the right to liberty and security. The right to the protection of personal data appears in the EU Charter of Fundamental Rights. [13]

The General Data Protection Regulation (GDPR), effective May 2018, provides a host of protections for the data relating to data subjects who reside within the EU. The GDPR is extraterritorial in application, protecting EU citizen data even outside the confines of the EU. Data controllers and processors will be required to meet criteria and abide by standards set forth in the GDPR in order to process personal and sensitive personal data. [14]

The GDPR arguably regulates a broad range of data, as it defines personal data as "any information relating to an identified or identifiable natural person…"[15] The Regulation provides additional clarity, specifying that personal data can include "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."[16] Sensitive personal data is defined in the Regulation as, "…personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data."[17]

The GDPR also arguably regulates a broad range of activities, as it defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means…" The Regulation goes on to specify that processing can include activities such as "…collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise

[13] (European Union, 2012)
[14] See Appendix A for relevant GDPR definitions
[15] (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016)
[16] (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016)
[17] (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016)

making available, alignment or combination, restriction, erasure or destruction…"[18] The Regulation also specifies that it covers processing inside and outside of the EU.[19]

While it is certainly true that the processing of personal data will occur when handling private information, it is imperative to understand that the GDPR can also govern public information. Publicly available information containing personal or sensitive personal data can still be subject to the protections of the GDPR.[20]

In order to process personal data, there must be a legal basis for doing so. The Regulation provides that data may be processed with the "freely given, specific, informed and unambiguous" consent from the data subject.[21] Other legal bases include but are not limited to, situations where processing is necessary for the performance of a contract, necessary for defense of legal claims, or where the processor has a legitimate interest that outweighs that of the data subject.[22]

Once a legal basis is established, there are still data protection principles that must be complied with in order to legally process data. These principles explicitly listed in the GDPR include: (1) lawfulness, fairness and transparency, (2) purpose limitation, (3) data minimization, (4) accuracy, (5) storage limitation, and (6) integrity and confidentiality.[23]

In the event that a legal basis for processing can be established and all data protection principles are complied with, data subjects are still entitled to protections under the GDPR. The GDPR gives data subjects the right to information about how their data will be processed, access to their data, the right to rectification to allow for the correction of errors, the right to erasure of their data and a number of others.

The GDPR places an additional hurdle on the cross-border transfer of data to a country outside of the EU, if that country to which the data is being transferred has been deemed to have inadequate data protection laws. A country is only considered to provide an adequate level of protection if they provide protections of essential equivalence to those protections in the EU.[24] The U.S.' privacy laws have been deemed inadequate. Therefore, in order to transfer the personal data of an EU data subject into the U.S., it must be done using one of a number of mechanisms.

The EU-U.S. Privacy Shield replaces the Safe Harbor scheme and allows for transfers from the EU to the U.S. companies. The Privacy Shield allows transfers for companies who meet a number of regulatory provisions within the agreement and certify that they will comply with data protection principles when handling the data of EU data subjects.[25]

In addition, companies can use contractual clauses either containing standard language previously approved by European data protection authorities, or contractual clauses not containing the

[18] (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016)
[19] (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016)
[20] (Dr. Michelle Frashner and Brian Agnew, 2016) at 30
[21] (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016)
[22] (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016)
[23] (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016)
[24] (Anna Myers, 2016)
[25] (Anna Myers, 2016)

standard language, which must be approved by data protection authorities prior to transferring data. For transfers between corporate entities or a group of corporate entities, Binding Corporate Rules subject to data protection authority approval is another mechanism for transfer of data.[26]

If none of the above can be employed, the GDPR lists derogations, meant to be narrowly construed, which would allow for transfer of data to a country without an adequacy decision. One such derogation allows personal data to be transferred upon receiving the consent of the data subject. The GDPR requires that the consent be explicit and given only after the data subject has been notified of the risks associated with transferring the data given the lack of adequate protections.

Storing personal data that falls under the governance of the GDPR also requires careful consideration of the Regulation. The GDPR imposes a requirement to keep the data secure. While the GDPR does not explicitly state what it means to keep data secure, it does indicate that encryption of some kind is necessary.[27] The GDPR also imposes data breach notification requirements on those companies storing personal data. Companies must notify supervisory authorities, and potentially the individuals whose data may have been impacted, of a potential data breach within 72 hours.[28] Storage and breach notification requirements are in addition to the purpose and storage limitations set forth in the six data protection principles for lawful processing, listed above.

The GDPR, and other regulations globally, gives data subjects a number of rights. In addition to being notified that data is being processed and the other protections laid out in the GPDR, data subjects are entitled to the following: Data subjects have the right to access data being stored, to rectify data that is inaccurate, to have data deleted or restrict processing altogether, to have their data sent to themselves or third parties, and to be notified if a company processing data sends it to a third party. In addition, the GDPR prevents data subjects from being profiled based on automated processing of their data. Companies that process data must also timely comply with the requests of data subjects.[29]

The Right to Be Forgotten, while it does not require any action on the part of a company conducting due diligence, still may have an impact on the process. The Right to Be Forgotten allows for the deletion of data at the request of the data subject. This data, often publicly available data on the internet, could be the data which would have been uncovered as part of due diligence or EDD searches.

United States

While the U.SSS. does not have an overarching, comprehensive privacy regime like many other countries, this is not to say that there are no privacy protections. Unlike the EU's approach where

[26] (Anna Myers, 2016)
[27] (Tanguy Van Overstraeten, 2016)
[28] (Tanguy Van Overstraeten, 2016)
[29] (Hickman, 2016)

protection of personal data is treated as a fundamental right, the U.S.' approach to data privacy is to treat personal data as property and protect it as such.[30]

The U.S. privacy regime can best be described as "…sectoral," a reference to fragmented, cross-governmental and industry-specific regulation."[31] Implied Constitutional privacy protections stemming from the First, Third, Fourth, Fifth and Fourteenth Amendment exist, along with state and federal regulations.[32] State-level regulations are restricted, of course, to that which falls within the jurisdiction of each state. Laws that require minimum data security standards and data breach notification laws exist on the state level—in some states. Those federal regulations that do exist to offer privacy protections apply only to specific sectors or narrowly defined types of data and circumstances.[33] The Gramm-Leach Bliley Act offers protection of narrowly defined financial information. There exists no comprehensive privacy scheme comparable to that of the EU General Data Protection Regulation.

International

It is worth noting that the countries in the EU are not the only countries with a comprehensive privacy law in place. Argentina, Uruguay, Costa Rica, Mexico and Peru have data protection laws similar to those of the EU.[34] China, the Czech Republic, Slovakia and a number of other countries' privacy laws provide for criminal liability for violations of certain provisions.[35] On the other hand, there are countries without any applicable privacy laws. Because the data protection schemes vary by country, can be complex, and like all laws, are ever changing, it is important to incorporate data privacy review into a robust compliance program.

Complying with AML/ABAC Regulations with Privacy Regulations in Mind

Privacy can come into play in a number of places throughout the due diligence and KYC processes. While the due diligence and KYC processes vary, similarities exist when it comes to privacy concerns. These concerns include the collection, transfer and storage of customer documentation and collection and transfer of customer's personal information.

The best approach for a company would be to employ a data privacy professional or attorney as part of the compliance team to provide counsel on potential data privacy implications throughout the due diligence process. An alternative approach would be for an institution's compliance and legal functions to work together to ensure that data privacy compliance is made a priority and appropriately acted upon.

[30] (Schwartz, 2013) at 2
[31] (Cunningham, 2016) at 422
[32] (Cunningham, 2016) at 422
[33] (Cunningham, 2016) at 423
[34] (White & Case, 2011)
[35] (Lexology, n.d.)

Prior to performing any type of due diligence, it is imperative to do a careful review and analysis of the privacy laws in the applicable jurisdiction. As indicated above, privacy laws are country specific and vary in complexity and breadth. Therefore, it is necessary to perform such a review and analysis on every country in which due diligence is conducted. The privacy professional should first examine the company's due diligence process and determine where privacy vulnerabilities lie. Generally speaking, a financial institution's KYC process and an international company's Foreign Corrupt Practices Act due diligence process is as follows:

First, customer identification documentation is collected along with other information provided by the customer. The information being collected is undoubtedly personal information. The company or financial institution will ask for the names and dates of birth of individual customers and business directors and beneficial owners. They will also ask for things like addresses, email addresses and occupational information. Financial institutions will ask for national identification numbers. The aforementioned types of information are without question protected by the GDPR, and are likely protected by privacy laws in a number of other countries.

The next step is to verify that the customer provided information that proves that the customer is who they say they are. Next, the financial institution will perform CDD by consulting additional sources to build upon the customer profile. For customers determined to be high risk, based on pre-determined criteria such as holding a political office or residing in a high-risk country, EDD will be performed. Open-source internet searching, commercial databases, government and sanctions list and similar resources will be used when conducting CDD and EDD. The purpose of both processes is to determine whether or not a customer account should be opened or, in the case of FCPA due diligence, a vendor should be contracted with.

The following will be an application of privacy laws to the due diligence process, assuming the company performing due diligence is a U.S. company and the customer from whom the company is collecting information resides in the EU. The EU GDPR is one of the more comprehensive privacy regimes in the world and can therefore show the many places privacy can come into play when a U.S. company is conducting due diligence on individuals abroad.

As exemplified above, the GDPR places requirements on the collection, transfer and storage of personally identifiable information. A customer, when tasked with sending identification documents and other personal information, should also be notified on the how their data will be processed and the purpose of the collection. At the same time, the customer should also provide their unambiguous, express consent to processing and transfer of their information. While other derogations for processing can be relied on, having evidence of the customer's express consent on file may avoid the headache of having to argue and justify relying on another exception. For example, if the company were to rely on the legitimate interest and a customer wanted to argue that the company did not truly have a legitimate interest, the company may have to defend the allegations. Even if the company ultimately wins, it will still cost time and money to defend and could potentially attract unwanted media attention and reputational damage.

The same is true of transfer. The U.S. has not been deemed as a country that provides adequate protection. Therefore, it is necessary to put in place a mechanism that will make the transfer of

personal data from the EU to the U.S. legal. Providing the requisite notifications and collecting the proper consent regarding transfer of personal data is likely the best method for complying with transfer requirements. Even if a company becomes a party to the Privacy Shield and certifies that they will adequately protect personal data, it is not a bad idea to have an alternative. After all, Safe Harbor was once a valid transfer mechanism and has since been invalidated. Asking a customer to provide consent to transfer personal data, while they are already providing consent to process their data, will not create any hardship and provides a second layer of protection should one method be called into question.

It is necessary to notify and receive the consent of every data subject whose personal data will be processed and transferred. It is also important to note that some countries' data protection laws treat sole proprietorships and certain other unincorporated entities with the same protections as individuals. Therefore, the information related to a sole proprietorship is entitled to the same safeguards as an individual's information and the appropriate steps must be taken in order to lawfully process such data.

Storage of a customer's documentation and personally identifiable information is also subject to privacy protections and therefore imposes a responsibility on those companies and financial institutions storing personal data. The GDPR will require that companies and financial institutions limit the amount of data being collected as part of due diligence to that which is necessary and only as long as it is necessary for the purpose for which it was collected. This vague standard can open a company up to scrutiny from authorities who may disagree with the company or financial institution's judgment. On top of the duty to limit the amount of data collected, a company must also protect the data being stored using means such as encryption. Should protective measures fail and customer or vendor information is compromised, a company may be under obligation to notify authorities and affected individuals of breaches. Therefore, it is necessary for a company or financial institution to have a process for this in place.

The collection of additional customer information from sources outside of what was provided by the customer also requires a privacy analysis. As indicated above, the collection and processing of any kind is regulated by the GDPR. Even publicly available personal information is subject to the protections of the GDPR. It is worth noting that publicly available personal information is also subject to protections under the privacy laws of other countries. This is not just the case in the E.U.

As mentioned in the above overview of the GDPR, notice of and consent to processing by the data subject is an outlined exception which would make processing of personal data lawful. Searches for additional information conducted in the due diligence and the EDD process will surely produce personal information. The discussion in the preceding paragraphs regarding lawful transfer and storage should also be heeded in this context.

Additional rights given to data subjects under the GDPR create an additional burden on the company that is collecting and storing personal data. These rights in particular are linked to the transparency principle requiring companies to notify data subjects whose data they process. Without notice that their data is being processed and for what purpose, data subjects would not be able to exercise the rights to which they are entitled. Here too it is necessary to have processes in

place for situations where data subjects wish to exercise their rights to access or correct their data, or another of their other enumerated rights.

Lastly, complying with privacy laws should not end with the company itself. A company should also ensure that third-party business partners with which they are seeking to engage in business are also complying with privacy regulations. Even in countries where data privacy laws would not find the company liable for third-party privacy violations, reputational harm could result.

Conclusions and Recommendations

Companies in the U.S. have a number of compliance obligations with which they must comply when it comes to conducting business internationally. Specifically AML and anti-corruption regulations, which require a company to conduct due diligence on those entities and individuals they intend to do business with, can conflict with international data privacy regulations.

Proper due diligence and knowing the customer or vendor a company is working with can lead to the prevention of corruption, money laundering and even terrorism. Failing to uncover the unlawful activity can lead to do criminal or civil liability, fines and reputational damage. Failing to treat data privacy compliance with the same duty of care as other compliance obligations can lead to the same consequences.

Data privacy laws, depending on the country, also impose criminal or civil liability and large fines for violations. The GDPR, for example, allows for fines of up to 5 percent of annual global revenue for violations.[36] Individuals, in addition to data protection authorities, can bring private legal action against a company or financial institution for violations of the GDPR. It is important for a company to ensure compliance with privacy laws not only to avoid liability, but also to avoid getting a reputation as being a company that does not respect the rights of individuals or their data.

A company or financial institution can minimize risk by recognizing the importance of data privacy compliance and incorporating into their robust compliance program. It is imperative to have a privacy expert within the compliance function to evaluate the impact of privacy laws on the due diligence and know your customer processes and to provide oversight to assure the recommendations are being complied with. Alternatively, the compliance function and legal functions should work closely together to ensure that privacy is a consideration in compliance. This notion should start at the top, by impressing upon the board of directors and company executives the importance of privacy compliance within AML and anti-corruption compliance programs.

[36] (Frasher, 2015)

Appendix A

European Union General Data Protection Regulation: Relevant Definitions[37]

"Controller"	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
"Personal Data"	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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.
"Processing"	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"Processor"	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
"Sensitive Personal Data"	Personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).

[37] (Dr. Detlev Gabel, 2016)

References

Anna Myers, C. C. (2016, January 19). *Top 10 operational impacts of the GDPR: Part 4 - Cross-border data transfers.* Retrieved from The Privacy Adviser- Westin Research Center: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/

Carol Stabile, C. (2016, September 20). Achieving Enterprise Risk When AML and Privacy Laws Conflict. *ACAMS Today*.

Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission. (2012). *A Resource Guide to the U.S. Foreign Corrupt Practices Act.* Department of Justice.

Cunningham, M. (2016, Fall). Complying with International Data Protection Law. *University of Cincinnati Law Review*, 421-450.

Dr. Detlev Gabel, T. H. (2016, July 22). *Chapter 5: Key definitions – Unlocking the EU General Data Protection Regulation*. Retrieved from White and Case- Publications and Events: http://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation

Dr. Michelle Frashner and Brian Agnew, M. (2016, July 1). Multinational Banking and Conflicts Among US-EU AML/CTF Compliance and Privacy Law: Operational & Political Views in Context. *SWIFT Institute*.

European Union. (2012). *EU Charter of Fundamental Rights.* Retrieved from European Commission: http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm

Federal Financial Institutions Examination Council Bank Secrecy Act/ Anti-Money Laundering InfoBase. (n.d.). *Customer Due Diligence-Overview*. Retrieved from Bank Secrecy Act Anti-Money Laundering Examination Manual : https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_013.htm

Federal Financial Institutions Examination Council, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation,. (2010). *Bank Secrecy Act Anti-Money Laundering Examination Manual.* Federal Financial Institution Examination Council.

Frasher, M. (2015, August 27). Data Privacy and AML Rules on a Transatlantic Collission Course. *American Banker*.

Gordon, M. R. (n.d.). U.S. and International Anti-Money Laundering Developments. *The International Lawyer: A Quarterly Publication of the ABA/ Section of International Law*.

Hickman, T. (2016, January 1). *Rights of Data Subjects under the GDPR*. Retrieved from Society for Computers and Law: http://www.scl.org

Lexology. (n.d.). *A Comparative Guide to Data Security Penalties in 20+ Jurisdictions*. Retrieved from Lexology: http://www.lexology.com/library/detail.aspx?g=b1c6fa73-d749-4b77-ab41-0f575687fa39

Office of the Comptroller of the Currency. (n.d.). *Bank Secrecy Act (BSA)*. Retrieved from U.S. Department of Treasury: Office of the Comptroller of the Currency: https://www.occ.gov/topics/compliance-bsa/bsa/index-bsa.html

Ross Marrazzo, D. J. (2015, August 25). Integrating privacy into AML practice. *ACAMS Today*.

Schwartz, D. J. (2013). *GW Law Scholarly Commons.* Retrieved from GW Law Faculty Publications & Other Works: http://scholarship.law.gwu.edu/faculty_publications/956

SIDLEY. (2016, May 19). *FinCEN Issues Final Rule on Customer Due Diligence Requirements for Financial Institutions.* Retrieved from SIDLEY: http://www.sidley.com/news/2016-05-19-banking-and-financial-services-update

Stuart P. Lott, B. B. (2016, July 20). *The "Fifth Pillar" of AML/BSA Compliance FinCEN Issues Final Rule for New Customer Due Diligence Requirements under the Bank Secrecy Act.* Retrieved from Bradley Financial Services Perspectives: https://www.financialservicesperspectives.com/2016/07/the-fifth-pillar-of-amlbsa-compliance-fincen-issues-final-rule-for-new-customer-due-diligence-requirements-under-the-bank-secrecy-act/

Tanguy Van Overstraeten, R. C. (2016, October). *Link Laters.* Retrieved from The General Data Protection Regulation- A Survival Guide: file:///C:/Users/hughesje/Downloads/TMT_DATA_Protection_Survival_Guide_Singles%20(1).pdf

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (2016). General Data Protection Regulation. *Official Journal of the European Union*.

White & Case. (2011, September 30). *White and Case Technology Newsflash*. Retrieved from From Habeas Data Action to Omnibus Data Protection: The Latin American Privacy (R)Evolution: http://www.whitecase.com/publications/article/habeas-data-action-omnibus-data-protection-latin-american-privacy-revolution