Advocates for International Development
Lawyers Eradicating Poverty

Data Protection Law in the USA

Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally
White and Case

Type: Legal Guide

Published: August 2013

Last Updated: August 2013

Keywords: Data Protection (US)

This document provides general information and comments on the subject matter covered and is not a comprehensive treatment of the subject. It is not intended to provide legal advice. With respect to the subject matter, viewers should not rely on this information, but seek specific legal advice before taking any legal action

Any opinions expressed in this document are those of the author and do not necessarily reflect the position and/or opinions of A4ID

Guide to data protection laws in the United States

Overview of US Data Protection Laws

In contrast to its European counterparts, the United States does not have one single data privacy framework or directive. Rather, United States data protection law is comprised of a patchwork of federal and state laws and regulations, which govern the treatment of data across various industries and business operations.

To comply with U.S. data privacy laws, non-profit organizations operating in the United States must look to and comply with *both* federal and state laws. Generally, federal statutes regulate the collection, storage and use of sensitive non-public personal information. State legislation, in contrast, generally regulates disclosure requirements after a security breach of non-public personal information occurs. To effectively guide non-profit organizations operating in the U.S., we provide an overview of the federal statutes most applicable to 501(c)(3) organizations, and a sampling of relevant state data privacy laws in select state jurisdictions with the most developed data protection standards, which also happen to be the jurisdictions where many non-profit organizations operate. Finally, we have also outlined briefly some standards and best practices that can guide a non-profit organization when determining its approach to data protection in the United States.

While we have provided an overview on some state laws, there may be additional state laws regulating specific non-profit operations depending on the location of the organization's activities and the state residency of the individuals whose data is collected. It is important for non-profit organizations to assess comprehensively their operations in the United States, and understand which state jurisdictions are regulating their activities. We recommend carefully reviewing the laws of each state from which you collect information or operate to ensure full compliance with the relevant laws and regulations.

Federal statutes may be enforced by federal government regulators or, if they include a private right of action, may be enforced through civil suits brought by individuals affected. State laws are likewise enforced by state regulators or, if a private right of action is included, by private citizens bringing civil suit.

This Guide focuses on the federal laws most likely to impact a non-profit's operations. Data privacy and data security is a dynamic area of the law in the United States, and is continuously changing. Moreover, although many federal statutes would not appear on initial review to apply to the charitable activities of many non-profit organizations, often either their operational terms are defined very broadly and also capture certain 501(c)(3) organizations or they may apply to some of the fund raising or other support activities of the non-profit organization. As such, we recommend continually monitoring legal developments in the

United States and regularly reassessing your organization's compliance with the law in light of changes in applicable regulations at both the federal and state levels.

Please note that we have not provided a glossary to this Guide, as the definition for many terms vary substantially from statute to statute.

Federal Laws

Federal data protection laws in the U.S. are primarily driven by industry and data type. With an increase in focus on data privacy and consumer protection in recent years, it is likely that data protection laws will be enforced more stringently by regulators in the near future. This section provides an outline of various federal statutes that may apply to non-profits. The FTCA, discussed first, prohibits unfair and deceptive practices, and requires all organizations to comply with any policies and procedures, made known to the public. Next, HIPAA and FERPA are discussed and are especially important for those organizations dealing with health-related or education-related data or records. The CAN-SPAM Act applies to most non-profits that send out "spam" solicitation messages to those not on a membership list. GBLA and the FRCA both regulate the treatment of consumer financial information. Finally, COPPA, though not binding on 501(c)(3) organizations, is a federal statute requiring notification and consent for online targeting of minors, and should be used as a guide for best practices for any non-profit engaged in online communications with those under the age of thirteen.

While a non-profit organization may not initially identify with some of the industries, activities, or data categories outlined and discussed below, organizations must carefully assess each of their operating activities to determine if any of their fundraising databases, client or customer contact lists, or project or issue-specific research for advocacy work might fall under the purview of one of these federal statutes.

1) Federal Trade Commission Act

The Federal Trade Commission Act[1] ("FTCA") was enacted to prohibit "unfair or deceptive acts or practices in or affecting commerce."[2] A trade practice is deceptive if it involves a "material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances, to the consumer's detriment."[3] The Federal Trade Commission ("FTC") has brought actions against companies, alleging deceptive acts, where the company failed to adequately protect consumers' information as promised under such companies' privacy

[1] 15 U.S.C. § 45, *et seq*.
[2] *Id*. at § 45(a)(1)
[3] Marcia Hofmann, *Federal Trade Commission Enforcement of Privacy*, *in* PROSKAUER ON PRIVACY 4:1.2[B] (2011), citing the Fed. Trade Comm'n, FTC Policy Statement on Deception, Letter from Fed. Trade Comm'n to Hon. John D. Dingell, Chairman, H. Comm. on Energy and Commerce (Oct. 14, 1983), ww.ftc.gov/bcp/policystmt/addecept.htm.

policies.[4] The FTC has also brought claims under this statute against companies that disclose customer information beyond the stated provisions in their privacy policies.[5]
In order to comply with the FTCA, organizations should not mislead consumers, customers or clients as to the use of their personal information, and should not otherwise exceed the scope of their privacy policies and notices given to their customers.

2) Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act [6] ("HIPAA") applies to all Covered Entities that collect, maintain, use, or disclose personal health information.[7] A Covered Entity is defined as a (1) health plan, (2) health care clearing house or (3) health care provider who transmits any health information in electronic form in connection with a transaction covered by the law.[8] Under HIPAA, Covered Entities must comply with the Privacy and Security Rules. Under the Privacy Rule, Covered Entities may not use or disclose Protected Health Information, except under specific circumstances or where authorized by the patient or participant. Under the Security Rule, Covered Entities are required to ensure the confidentiality, integrity and availability of *electronic* Protected Health Information that they maintain or transmit, by enforcing reasonable and appropriate administrative, physical and technical safeguards.[9]

Under the Health Information Technology for Economic and Clinical Health Act[10] ("HITECH Act"), the Privacy and Security Rules of HIPAA are extended and directly apply to "Business Associates" that work with Covered Entities and access PHI.[11] A Business Associate is defined as "a person who (i) on behalf of such covered entity…performs or assists in the performance of (A) a function or activity involving the use or disclosure of individually identifiable health information…"[12] Business Associates are therefore directly liable for any violations of the Privacy and Security Rules, and may be prosecuted for data privacy violations.[13] Therefore, any non-profit organization that works with a Covered Entity may be subject to HIPAA regulations.

---

[4] Decision and Order, Petco Animal Supplies, Inc., FTC File No. 032-3221 (2004) (Petco assured consumers that it took measures to protect against unauthorized access to consumer information, but failed to implement these security measures).
[5] Complaint, *FTC v. Rennert, International Outsourcing Grp., Inc., et al.*, CV-S-00-0861-JBR (D. Nev. 1999) (FTC File No. 992-3245), www.ftc.gov/os/2000/07/iogcomp.htm.
[6] 45 C.F.R. § 160 *available at* http://www.legalarchiver.org/hipaa.htm.
[7] *Id.* at § 160.102.
[8] *Id.* at § 160.104.
[9] *Id.* at §§ 164.302-.318.
[10] 42 U.S.C. §§ 300jj (2009), *et seq*.;1709 (2009), *et seq*, *available at* http://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra.pdf.
[11] 45 CFR 160.103.
[12] *Id*.
[13] 75 Fed. Reg. 40872.

3) Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act[14] ("FERPA") protects the data included in students' educational records, and applies to all educational agencies and institutions that receive applicable funding from the U.S. Department of Education, including non-profits.[15] Under this law, "educational records" are defined as records, files, documents, and other materials that contain information directly related to a student that are maintained by an educational agency or institution or by a person acting for such agency or institution.[16] An educational agency or institution is defined as any public or private agency or institution which is the recipient of funds under any applicable government program.[17]

Under FERPA, any school that receives educational funding from the government must provide parents of students, or the students themselves if they are over the age of eighteen, with the right to inspect and review the student's educational records. Each educational agency or institution is required to establish appropriate procedures for granting such requests within a reasonable time, but in no case more than forty-five days after the request is made.[18] In addition, FERPA requires the educational agency or institution to obtain written consent from a parent, guardian or eligible student before releasing education records or personally identifiable information contained therein to any individual, agency or organization, other than to a list of specifically excluded individuals and related state agencies or officials.[19]

If an educational agency or institution wishes to publish "Directory Information," relating to the student's name, address, telephone number, date and place of birth, field of study, activities, dates of attendance, degrees, awards and institution attended by the student, the agency or institution must first give public notice of the categories of information it designates to make public and allow a reasonable time for a parent to inform the agency or institution that it wishes to not release such information without prior consent.[20]

Finally, under FERPA, educational agencies or institutions are required to keep records which indicate all individuals, agencies or organizations that have requested or obtained access to a student's records, including the interest that each such third-party has in the student's information.[21] This record must be available only to parents, school officials and individuals responsible for maintaining such records. Such personal information may only be transferred to third-parties on the condition that such party will not permit any other party to have access

---

[14] 20 USC § 1232g, *available at* http://www.gpo.gov/fdsys/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20-chap31-subchapIII-part4-sec1232g.pdf.
[15] *Id.* at § 1232g(a)(3).
[16] *Id.* at § 1232g(a)(1)(D)(3).
[17] *Id*.
[18] *Id.* at § 1232g(a)(1)(A).
[19] *Id.* at § 1232g(b).
[20] *Id.* at § 1232g(a)(5)(A).
[21] *Id.* at § 1232g(a)(4)(A).

to such information without the written consent of the parents or the eligible student.[22] There is no private cause of action under FERPA, however, its provisions may be enforced by the Secretary of Education.[23]

4) Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)

The Non-Solicited Pornography and Marketing Act of 2003[24] ("CAN-SPAM Act") regulates commercial email messages. Commercial email messages are defined as any email message, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service. However, emails that include a "transactional or relationship message" are excluded from the definition of commercial email message and are not subject to the provisions in the CAN-SPAM Act.[25]

Pursuant to the CAN-SPAM Act, all organizations, including 501(c)(3) organizations, must not send emails with materially false, misleading or deceptive information in the header or subject line.[26] Thus, if an email is an advertisement or solicitation, it must clearly identify itself as such. The email must contain "clear and conspicuous" notice of the opportunity to opt-out of receiving future emails from the sender, and must include some type of return email address or other mechanism whereby the recipient is in fact able to opt-out.[27] The email must contain a valid, physical postal address of the sender. Finally, senders must respect the decisions by recipients to opt out from receiving any such future emails from the sender.[28]

It is important to note that 501(c)(3) organizations may still email large groups of people if those messages are related to the non-profit's mission and include information for members or for those whom the non-profit has had a transactional relationship, such as donors.[29] The CAN-SPAM Act is enforced by the FTC, pursuant to its authority to prevent unfair and deceptive trade practices under the FTCA.[30] In addition, State Attorney Generals can enforce the law, as it preempts other state laws regarding unsolicited commercial email communications.

5) Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act[31] ("GLBA") requires that financial institutions "respect the privacy of its customers and protect the security and confidentiality of those customers' non-public

---

[22] *Id.* at § 1232g(a)(4)(B).
[23] *Id.* at § 1232f.
[24] 15 U.S.C. §§ 7701 (2003), *et seq*, *available at* http://uscode.house.gov/download/pls/15c103.txt.
[25] *Id*. at § 7702.
[26] *Id*. at §§ 7704(a)(1)-(2).
[27] *Id*. at § 7704(a)(3).
[28] *Id*. at § 7704(a)(4).
[29] *See* FED. TRADE COMM'N, THE CAN-SPAM ACT: A COMPLIANCE GUIDE FOR BUS. 2 (2009), *available at* http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business.
[30] 15 U.S.C. § 7706.
[31] *Id.* at § 6801, *et seq.*

personal information."[32] Financial institutions are broadly defined as "any institution the business of which is engaging in financial activities as described in section 1843(k) of Title 12."[33] While 501(c)(3) organizations are not particularly enumerated as a class that is liable under the GLBA, non-profit organizations that engage in financial activities and are regulated by Federal functional regulators, state insurance authorities, or the FTC would be included.[34] Therefore, 501(c)(3) organizations deemed "financial institutions and other persons subject to their jurisdiction under applicable law" must comply with the GLBA.[35] We recommend that you investigate whether your organization would be deemed to be a "financial institution" under the GLBA. This is a fact intensive inquiry, and we advise you to look closely at this with your legal advisors.[36] "Non-public personal information" is defined in the statute as "all personally identifiable financial information "(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service provided for the consumer; or (iii) otherwise obtained by the financial institution."[37]

To comply with GLBA, the financial institution must provide "clear and conspicuous"[38] disclosure of (1) policies concerning disclosing non-public information to affiliated and nonaffiliated entities, (2) categories of non-public personal information collected by the institution, and (3) policies in place to protect confidentiality and security of non-public personal information.[39] In addition, financial institutions are required to provide customers with annual notice of their privacy policies and of the right to opt-out from sharing personal information with non-affiliated third parties.[40] The financial institution must disclose their privacy policy "at the time of establishing a customer relationship with the consumer *and* not

---

[32] *Id*. at § 6801(a).

[33] *Id*. at.§ 6809(3)(A). To determine whether an entity is a "financial institution," courts may consider the following factors: "(A) the purposes of this chapter and the Gramm-Leach-Bliley Act; (B) changes or reasonably expected changes in the marketplace in which financial holding companies compete; (C) changes or reasonably expected changes in the technology for delivering financial services; and (D) whether such activity is necessary or appropriate to allow a financial holding company and the affiliates of a financial holding company to— (i) compete effectively with any company seeking to provide financial services in the United States; (ii) efficiently deliver information and services that are financial in nature through the use of technological means, including any application necessary to protect the security or efficacy of systems for the transmission of data or financial transactions; and (iii) offer customers any available or emerging technological means for using financial services or for the document imaging of data." 12 U.S.C. § 1843(k)(3).

[34] "Federal functional regulators" consist of six entities: (1) the Board of Governors of the Federal Reserve System; (2) the Office of the Comptroller of the Currency; (3) the Board of Directors of the Federal Deposit Insurance Corporation; (4) the Director of the Office of Thrift Supervision; (5) the National Credit Union Administration Board; and (6) the Securities and Exchange Commission. 15 U.S.C. §§ 6809(2)(A)-(F).

[35] 15 U.S.C. § 6805(a).

[36] The determination of whether an organization constitutes a "financial institution" is beyond the scope of the Guide and involves a fact-intensive inquiry, individual to each organization. Organizations whose activities are particularly financial in nature and involve, for example, micro-lending schemes or investment vehicles, are especially advised to work with counsel to determine whether their nonprofit meets the definition of "financial institution" under federal law.

[37] *Id*. at §§ 6809(4)(A)(i)-(iii).

[38] *Id.* at § 6803(a).

[39] *Id*. at §§ 6803(c)(1)-(3).

[40] *Id.* at § 6802.

less than annually during the continuation of such relationship."[41] Such notice may be sent by mail or e-mail.[42] Therefore, customers or clients that share information with a non-profit meeting the definition of "financial institution," whether sharing such information in person or online, must be presented with the non-profit's privacy policy. All customers or clients that the non-profit maintains an ongoing relationship with should be provided copies of the organization's privacy policy annually, whether by mail or e-mail. This would likely mean customers or clients who provide financial information for periodic giving campaigns, whose financial information is registered with the organization for the purpose of one-off fundraising or online auction-bidding at fundraisers, and those whose non-public financial information is kept by the organization due to repeat purchases or for billing purposes.

To comply with GLBA with respect to the handling of non-public financial information, financial institution organizations must (1) appoint an employee to manage the information security program, (2) identify reasonably foreseeable risks to consumer information, establishing and implementing safeguards to control the risks, regularly monitoring the effectiveness of the safeguards; (3) require service providers by contract to protect consumer information and (4) assess and adjust the information security program when necessary.[43] There is no private right of action under this statute; only government regulators may enforce the GLBA.[44]

6) Fair Credit Reporting Act

The Fair Credit Reporting Act[45] ("FCRA") was enacted to promote fair and accurate credit reporting, and establishes procedures for the collection, use and protection of personal information held by "Consumer Reporting Agencies,"[46] typically shared through the issuance of "Consumer Reports."[47] FCRA applies for the most part only to "Consumer Reporting Agencies" who provide "Consumer Reports." A Consumer Rating Agency is defined as any person who, whether for monetary reasons or on a non-profit basis, regularly engages in "the practice of assembling or evaluating consumer credit information … for the purpose of furnishing consumer reports to third parties."[48] Any person or entity that engages in "assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties" is a Consumer Reporting Agency, for purposes of the statute.[49] The meaning of Consumer Reporting Agency has historically been interpreted quite broadly.[50] For this reason, even non-profit organizations who may not meet the definition of "financial institution" under the GBLA may still be bound

---

[41] *Id*. at § 6803(a).
[42] *Id*.
[43] 16 C.F.R. §§ 314.4(a)-(e).
[44] 15 U.S.C. § 6805(a).
[45] 15 U.S.C. § 1681, *et seq.*
[46] *Id*. at § 1681a(p).
[47] *Id.* at § 1681a(d)(1).
[48] *Id.*at § 1681a(f), *available at* http://www.ftc.gov/os/statutes/031224fcra.pdf.
[49] *Id*.
[50] Kristen J. Mathews & Christopher Wolf, *Financial Privacy Law*, *in* PROSKAUER ON PRIVACY § 2:2.2[C] (2011).

by FCRA. As a result, if a non-profit is directly collecting information from consumers for purposes of creating risk and credit profiles that are then shared among the affiliated entities, each collecting and compiling entity within the organization would be considered a separate Consumer Reporting Agency.

A Consumer Report is defined as a written, oral, or other communication by a consumer reporting agency "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used to or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance."[51] There are, however, some notable exceptions to the definition of a Consumer Report. For example, Consumer Reports specifically do not include: (i) a report containing information solely as to transactions between the consumer and the person making the report; (ii) communication of information as to a specific transaction between the consumer and person making the report, shared with affiliates; or (iii) communication of any information among affiliates, if it is clearly and conspicuously disclosed to the consumer that such information may be shared with affiliates, and the consumer is given notice and opportunity to direct that such information not be shared.[52]

It is important to note that if a non-profit organization intends to obtain Consumer Reports from a third party Credit Reporting Agency, such as Experian or Equifax, there are limits on the organization's use of such consumer information. FCRA requires that Consumer Reports and the information contained therein only be furnished by Consumer Reporting Agencies for use in specific circumstances, such as in response to court order or legal process, pursuant to written instructions from the particular consumer, or to a third party who intends to use the information for considering whether to extend credit to a consumer or determine the consumer's eligibility for employment or a license or otherwise for a legitimate business purpose with a business transaction initiated by the consumer. [53] Similarly, most data providers, such as Credit Reporting Agencies, limit the ability of a purchaser to share reports, even with affiliated entities, so reference should be made to an organization's contracts with the Consumer Reporting Agencies it works with so as to avoid potential breach liability.

FCRA also regulates disclosures by any person, not just Consumer Reporting Agencies, of customers' financial information, between affiliates, for marketing purposes. Pursuant to the FCRA, an entity may not use information in the Consumer Report for marketing purposes *unless* "(A) it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons for purposes of making such solicitations to the consumer; and (B) the consumer is provided an opportunity and a simple method to prohibit the making of such solicitations to the consumer by such person."[54] Therefore, an organization may share financial information with affiliates or subsidiaries for marketing

[51] *Id*. at. §§ 1681a(d)(1), 1681a(f), *available at* http://www.ftc.gov/os/statutes/031224fcra.pdf.
[52] *Id*. at §§ 1681b(2)(A)-(B).
[53] *Id.* at §§ 1681b(a)(1)-(6).
[54] *Id*. at § 1681s-3(a)(1).

purposes only where (1) the consumer is given clear notice that information will be shared and (2) the consumer had an opportunity to opt out, and has not done so.[55] Notice must be delivered "so that each consumer can reasonably be expected to receive actual notice,"[56] and the consumer must be provided a reasonable opportunity to opt out.[57] The opt out is effective for five years.[58]

If a company fails to provide the customer with notice and an opportunity to opt out, that company is prohibited from sharing such information, beyond the statutorily "permissible purposes" outlined in FCRA. "Permissible purposes" are narrowly defined, and include disclosure (1) in response to court order, (2) in response to written instructions from the data-owning consumer, or (3) upon request, to relevant federal and state agencies and officials.[59] If a company discloses protected information to its affiliate without complying with FCRA, both the disclosing entity and the affiliate who accesses such information will be in violation of FCRA.

There is a private right of action for willful noncompliance, knowing noncompliance and negligent noncompliance with the FCRA.[60] Because of the broad interpretation of "Consumer Reporting Agency," the provisions preventing disclosure of customer financial information for by *any* person, and the available private right of action that would allow an individual citizen to sue in the event of a breach, the FCRA has the potential to be broadly applied and non-profit organizations should be careful to review their financial information retention and disclosure policies.

7) Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act ("COPPA")[61] was enacted to protect children under the age of thirteen in their use of the Internet by regulating how websites collect, use, and disclose children's personal information. Under COPPA, before a website "operator"[62] may collect a child's personal information, it must notify the child's parent of its data collection practices and must obtain parental consent to collect the information.[63] COPPA applies to operators of websites directed to children and to "general audience" websites if the operator has actual knowledge that the website is collecting children's personal

---

[55] *Id*.

[56] The notice requirement is satisfied (1) by mailing a copy to the consumer's last known address or (2) by email, provided the consumer agreed to receive electronic disclosures, or (3) by posting the notice on an internet website where the consumer obtained the product or service, provided the consumer is required to acknowledge receipt of the notice. 12 C.F.R. § 41.26.

[57] *Id.*at §§ 41.24, 41.26. The "reasonable opportunity" provision may be satisfied by providing customers with (1) a check-off box, on documents they receive, (2) a form, with a pre-printed reply and self-addressed envelope, (3) electronic means to opt-out or (4) a toll-free telephone number to opt out.

[58] *Id.* at § 41.22(b).

[59] 15 U.S.C. §§ 1681b(a)(1)-(6).

[60] *Id*. at §§ 1681n(a), 1681n(b), 1681o(a).

[61] 15 U.S.C. §§ 6501, *et seq*, *available at* http://www.coppa.org/coppa.htm.

[62] 16 C.F.R. pt 312.2.

[63] *Id.* at pts. 312.4(c), 312.5.

information.[64] Although COPPA does not apply to non-profit organizations, we recommend as best practices, that any organization that collects information from children under the age of thirteen first obtain parental consent.[65]

State Laws

Nearly every state has enacted some form of data privacy law applicable to its jurisdiction. It is important to note that while state data privacy laws apply, respective State Attorneys General may sue for violation of federal law as well. Therefore, non-profit organizations should not view federal and state statutes as two separate jurisdictional spheres, but rather as sets of laws that would be applied in concert with each other.

Generally, data privacy law in most states is focused on breach notification, with entities required to notify consumers whose personal information is compromised. The notable exceptions are California and Massachusetts, which have laws and regulations in place that are more proactive and farther reaching. It is important to note that California and Massachusetts enacted laws that apply to any entity, anywhere in the United States, with access to non-public information of one of their residents. Because of the forward-looking nature of both California and Massachusetts data privacy laws, these states are included as a primary focus in this Guide, and can provide a good indication of the maximum requirements of data privacy law compliance in the United States. In addition, specific data privacy regulations in both New York and the District of Columbia are included, as many non-profit organizations have operations based in these jurisdictions.

California

We recommend that all non-profits operating in the U.S. comply with California data privacy laws. First, if the non-profit wishes to engage in fundraising in the United States, it is likely that at least one of the donors whose information is being collected will be resident of California, and thus subject to the state's data privacy protections. Second, with technology-focused industries at the center of the state's economy, there is increasingly ardent support by California residents for strong data privacy protections: a non-profit looking to engage with the California public may enhance its appeal by demonstrating awareness of this issue. Finally, data protection is increasingly a hot button issue in the state and enforcement of data privacy laws is increasing.

California is seen as a leader among the states in connection with data privacy issues. By complying with California data privacy regulations, a non-profit may find itself also complying with the data privacy regulations emerging in other state jurisdictions.

---

[64] *Id.* at pt. 312.3.
[65] 15 U.S.C. § 6501(2)(B).

1) California Online Privacy Protection Act

The California Online Privacy Protection Act[66] ("Cal. COPPA") requires operators of commercial websites or online services that collect personally identifiable information through the Internet about consumers residing in California, who use or visit their websites or online services, to "conspicuously" post a privacy policy on their website.[67] Personally identifiable information is defined as "individually identifiable information about an individual consumer collected online by the operator form that individual and maintained by the operator in an accessible form." This is a broad definition of information, and explicitly includes data, such as the consumer's first and last name, home or other physical address, e-mail address, telephone number, social security number, as well as information concerning a user that the Website or online service collects online from the user and maintains in personally identifiable form in combination with an identifier, such as those listed above.[68]

In order to comply with Cal. COPPA, the privacy policy must (i) identify categories of personal information collected, (ii) identify all third parties with whom the operator may share personal information, (iii) describe the process (if any) for customers to review and request changes to the personal information collected, and (iv) identify the effective date of the privacy policy.[69] Due to the broad definition given to "personally identifiable information" and the specifically enumerated requirements for an organization's privacy policy, 501(c)(3) organizations operating a website that collects information from a California resident – whether intentionally or not – should carefully assess their current policies in light of the requirements. Organization leaders should undertake a fact-driven analysis to determine whether their current activities apply with Cal. COPPA, as those organizations with broad membership and mission scope are likely to reach a California resident, and thus be liable under Cal. COPPA. Enforcement of Cal. COPPA over the last year has increased dramatically, with the State of California Attorney General ("CA AG") raising complaints against companies whose mobile applications fail to include a privacy policy. Those non-profit organizations with mobile applications or other electronic communications tools beyond websites are advised to review the CA AG's website for up to date information on data privacy priorities in this area.[70]

2) California Financial Information Privacy Act

The California Financial Information Privacy Act[71] ("CFPIA") prohibits financial institutions from sharing or selling personally identifiable non-public information without obtaining the

---

[66] Cal. Bus. & Prof. Code § 22575 (2006), *et seq*, *available at* http://oag.ca.gov/privacy/COPPA.
[67] *Id*. at § 22575(a).
[68] *Id*..
[69] *Id*. at § 22575 (b).
[70] *See also* CALIFORNIA DEPARTMENT OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (January 2013), http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.
[71] Cal. Fin. Code § 4050 (2012), *et seq*, available at: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=fin&group=04001-05000&file=4050-4060.

consumer's consent.[72] The CFPIA's defines a "financial institution" as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 of the United States Code and doing business in this state."[73] This definition includes those financial activities provided under GLBA, discussed above. "Non-public personal information" is defined as personally identifiable information, either: (1) provided by a consumer to a financial institution, (2) resulting from any transaction with the consumer or any service performed for the consumer, or (3) otherwise obtained by the financial institution.[74]

In order to share any non-public personal information with an unaffiliated third party, the financial institution is required to obtain consent in writing, dated and signed by the consumer that clearly and conspicuously states that by signing, the consumer is consenting to the disclosure of his or her non-public personal information to third parties. The form must also say that this consent, if given, can be revoked or modified at any time, and must include information on procedures for revoking such consent.[75] In order to share any non-public personal information with an affiliated party, the financial institution must clearly and conspicuously notify the consumer annually in writing that the non-public personal information may be disclosed to an affiliate, and that the consumer has not directed that this information not be disclosed. This notice must inform the consumer that the consent will remain in effect until revoked, that the consumer may revoke consent at any time, and provide information to the consumer on how to revoke such consent.[76] This statute may be enforced by the state attorney general; there is no private right of action.[77]

Though many non-profit organizations may not view themselves as engaging in financial activities, CFPIA is likely applicable to those organizations engaged in the following areas: micro-lending; community lending services; local or international banking, budgeting or investment training initiatives; social impact investing or social impact bonds; and other actions requiring the organization to directly hold securities. For organizations engaged in such activities, particular attention should be paid to CFPIA but also to federal statutes regulating the protection of non-public financial information, such as GBLA or FCRA. Prudent planning with financial advisory and tax legal professionals is also recommended.

3) California Shine the Light Law

Pursuant to the California Shine the Light Law[78], any organization – including non-profits – that transfer personal information to third parties for direct marketing purposes, is required to disclose their data sharing practices with any California resident who requests such

---

[72] *Id*. at § 4052.5.
[73] *Id*. at § 4052(c). This definition is identical to the "financial institution" definition under GLBA. 15 U.S.C. § 6809(3)(A).
[74] *Id*. at § 4052(a).
[75] *Id*. at § 4053(a)(2).
[76] *Id*. at § 4053(b)(1).
[77] *Id*. at § 4057.
[78] Cal. Civ. Code § 1798.83, *et seq*, *available at* http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84.

information, free of charge.[79] Specifically, the organization must provide the resident, in writing or by email, a list of categories of personal information disclosed to the third party during the immediately preceding calendar year and the names and addresses of all third parties receiving such information.[80] Organizations are required to designate a mailing address, email address or telephone number to which customers may request such information.[81]

Personal information is broadly defined as any information that, when it was disclosed, identified or described, was able to be associated with an individual, and includes – but is not limited to - all of the following types of information: (a) individual's name and address; (b) email address; (c) age or date of birth; (d) names of children; (e) e-mail or other addresses of children; (f) number of children; (g) age or gender of children; (h) height; (i) weight; (j) race; (k) religion; (l) occupation; (m) political party affiliation; (n) real property purchased, leased or rented; (o) credit or debit card number; (p) bank or investment account, debit or credit card balance.[82]

Although this law applies to non-profits, the law is limited to information that is shared for "direct marketing purposes." The definition of "direct marketing" specifically excludes the use of personal information by a bona fide tax exempt charitable or religious organization to solicit charitable contributions.[83] Therefore, when a registered non-profit shares information for the purposes of soliciting charitable contributions, the organization is not required to comply with the California Shine the Light Law.

Massachusetts

Massachusetts takes a uniquely proactive approach to data protection and has instituted minimal data privacy requirements for any person, corporation, association, partnership or other legal entity that maintains personal information about Massachusetts residents.[84] This regulation applies to registered non-profits. Pursuant to Massachusetts' data privacy laws, all organizations that possess sensitive personal information about Massachusetts residents must adopt a compliant Information Security Program to protect that information.[85] Personal information is defined in the statute as a resident's first and last name, or first initial and last name, *in combination with* the resident's social security number, driver's license or state identification number or financial account number.[86]

---

[79] *Id*. at 1798.83(a).
[80] *Id*. at 1798.83(a)(1).
[81] *Id*. at 1798.83(b)(1).
[82] *Id*. at 1798.83(e)(7).
[83] *Id*. at 1798.83(e)(2)(A).
[84] 201 CMR § 1700 (2010), *et seq*, *available at* http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.
[85] *Id*. at § 1705.
[86] *Id*. at § 1702 (emphasis added).

According to Massachusetts' *Standards for the Protection of Personal Information of Residents of the Commonwealth*, all organizations must identify and assess risks to confidentiality, develop an appropriate security policy, and regularly monitor the security program.[87] Massachusetts requires that the organization designate an employee to maintain the security system. The organization must review the scope of the security measures annually. The organization must impose disciplinary measures for security violations and document any actions taken in response to a breach of security.[88]

New York

1) Information Security Breach and Notification Act

Pursuant to New York's General Business Law § 899-aa, any individual or company that conducts business in New York state and owns or licenses computerized data, which includes private information, is required to disclose any breach of the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.[89] Private information is defined as personal information, such as an individual's name, number, personal mark or other identifier used to identify such person in combination with one or more of the following data elements: social security number, driver's license number or non-driver identification card number or account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.[90]

In the event that the organization has to provide notice to any New York state resident, such organization must also notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons.[91] If more than five thousand New York residents are to be notified at one time, the organization must also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of persons affected.[92] The state attorney general enforces this law, and pursuant to this section, is permitted to bring a cause of action against any organization that fails to comply with this breach notification law.[93]

---

[87] *Id.* at §1703.
[88] *Id*.
[89] N.Y. Gen. Bus. Law § 899-aa, *et seq, available here*.
[90] *Id*. at §§ 899-aa(1)(a)-(b).
[91] *Id*. at § 899-aa(7)(a).
[92] *Id*. at § 899-aa(7)(b).
[93] *Id*. at § 899-aa(6)(a).

2) Social Security Number Protection Law

This law prohibits organizations from disclosing an individual's unencrypted social security number to the public, printing the social security number on any card or tag required to access products, services or benefits, requiring an individual to transmit their social security account number over the internet, or printing a social security number on materials that are mailed to the individual, unless required by law.[94] Under this law, a Social Security Account Number is defined as the number issued by the federal social security administration, as well as *any number derived therefrom*, such as the last four digits.[95] The state attorney general is permitted to enforce this law, and there is no private cause of action.[96]

District of Columbia

The District of Columbia has enacted the Consumer Personal Information Security Breach Notification Act[97], which requires any organization that conducts business in D.C., and who owns or licenses computerized or other electronic data, to notify any resident whose personal information is affected in a security breach.[98] If the organization is required to notify more than one thousand people, that organization must also notify all consumer reporting agencies of the timing, distribution and content of the notices sent out to individuals.[99] This law may be enforced by both private individuals affected by the security breach and the attorney general.[100]

Personal information is defined as an individual's first name or first initial and last name, or phone number or address, in combination with one or more of the following data elements: social security number, driver's license number or District of Columbia Identification Card number, or credit card number or debit card number, or any other number or code or combination of numbers or codes, such as an account number, security code, access code or password that allows access to or use of an individual's financial or credit account.[101]

---

[94] N.Y. Gen. Bus. Law §§ 399-dd(2)-(3).
[95] *Id*. at § 399-dd(1)(a).
[96] *Id*. at § 399-dd(7).
[97] D.C. Code §§ 28-3851 – 28-3853, *available at* http://dc.gov/DC/Government/Data+&+Transparency/Consumer+Protection/Consumer+Information+101/Consumer+Personal+Information+Security+Breach+Notification+Act.
[98] D.C. Code § 28-3852.
[99] *Id*.
[100] *Id*. at § 28-3853.
[101] *Id*. at § 28-3851(3)(a).

Other Revelant Regulations

In addition to the above listed federal and state laws, the following standards and frameworks may be relevant to non-profits operating in the U.S. As discussed below, the PCI DSS provides a roadmap for best practices in handling sensitive credit card information. This can be particularly important for organization routinely receiving payments, such as donations, online. Additionally, for non-profits based outside the U.S., there may be a safe harbor framework in place to ensure that your organization is compliant.

1) Payment Card Industry Data Security Standard (PCI DSS)

Though not federal statute, the Payment Card Industry Data Security Standard ("PCI DSS") is a proprietary national standard for organizations handling credit card information. PCI DSS applies to all entities involved in payment card processing, as well as all entities that store, process or transmit cardholder data. PCI DSS contain a set of minimum requirements for protecting cardholder information, and are comprised of twelve standards requirements:

i. Install and maintain a firewall configuration to protect cardholder data
ii. Do not use vendor-supplied defaults for system passwords and other security parameters
iii. Protect stored cardholder data
iv. Encrypt transmission of cardholder data across open, public networks
v. Use and regularly update antivirus software or programs
vi. Develop and maintain secure systems and applications
vii. Restrict access to cardholder data by business need to know
viii. Assign a unique ID to each person with computer access
ix. Restrict physical access to cardholder data
x. Track and monitor all access to network resources and cardholder data
xi. Regularly test security systems and processes
xii. Maintain a policy that addresses information security for all personnel

For more information on PCI DSS compliance, please refer to www.pcisecuritystandards.org for more information.

2) U.S. – EU Safe Harbour Framework

The U.S. Department of Commerce along with the European Commission created a "Safe Harbor" framework, which enables U.S. companies to self-certify that they are compliant with EU standards for privacy protection. Companies that comply with the Safe Harbor are permitted to freely transfer data between the countries. Currently, twenty-seven Member States of the EU are party to the Safe Harbor Framework. EU organizations can ensure they are sending information to Safe Harbor compliant U.S. organizations by viewing the public list of companies posted on the Safe Harbor website.

Organizations may join the Safe Harbor voluntarily. Those that do so must comply with the Safe Harbor's requirements and publicly declare such. Organizations self-certify to the Department of Commerce annually in writing, and state in their privacy policies that they adhere to the Safe Harbor requirements. In the United States, the Safe Harbor declarations are enforced by the FTC, pursuant to the FTCA (discussed above), which prevents unfair and deceptive trade practices. Pursuant to this framework, any claims by European citizens against U.S. organizations will be heard in the United States, with some exceptions.

Companies qualify for the Safe Harbor by either joining a self-regulatory privacy program or by developing their own self-regulatory privacy policies that satisfy the seven Safe Harbor requirements. The Safe Harbor requires compliance with the following seven key principles:

- Notice: Organizations must notify individuals about why information is collected, how it is used, with whom such information is shared and how such information is protected. Organizations must also provide information on how individuals can contact the organization with inquiries and complaints.
- Choice: Organizations are required to give individuals the right to opt-out from programs in which their data is disclosed to a third party or used for a purpose incompatible with the purpose for which the data was originally collected or authorized. Choice also requires that users be given the option to opt-in when sensitive information will be disclosed to a third party for a purpose incommensurate with the original authorized purpose.
- Onward Transfer: Third-parties to whom information might be transferred are required comply with the Safe Harbor or other adequate data privacy protection measures.
- Access: Users must be given access to their personal information and be able to amend or correct information, provided that the costs of doing this are reasonable and no other individual's rights are affected.
- Security: Organizations must take reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, or destruction.
- Data Integrity: Personal information must only be used for relevant purposes.
- Enforcement: Organizations must have in place affordable and accessible mechanisms to investigate complaints and disputes; established procedures for verifying compliance to Safe Harbor principles; and an obligation and commitment to remedy problems arising from failures to comply with the Safe Harbor principles.

For more information on the US-EU Safe Harbor Framework, please visit here.

3) Cross-Border Privacy Rules System (US-APEC)

The U.S. joined the Cross-Border Privacy Rules System (CBPR System) on June 26, 2012. The CBPR System is an initiative by the Asia-Pacific Economic Cooperation (APEC) in which

organizations voluntarily agree to certain benchmark privacy policies and procedures, and are permitted to freely transfer data across borders.

These policies and procedures must be evaluated by an APEC-recognized Accountability Agent for compliance with CBPR guidelines. Once an organization is certified, the privacy policies and procedures become binding as to that participant and are enforceable by a defined authority to ensure compliance with the CBPR rules. The CBPR consists of the following four key elements:

- Self-assessment: An organization may use the APEC-recognized questionnaire which is provided by an APEC-recognized Accountability Agent. The questionnaire asks basic questions about notice, collection limitations, uses of personal information, choice mechanisms, integrity of personal information, security safeguards, access and correction, and accountability.
- Compliance Review: The questionnaire is then submitted to the Accountability Agent who performs the compliance review to ensure that the minimum CBPR requirements are satisfied.
- Recognition/Acceptance: If the organization satisfies the CBPR requirements, this information is then made publicly accessible in a directory which allows consumers to contact participating organizations, as well as information on the Agents who certified each organization and the relevant Privacy Enforcement Authority they can seek for redress of complaints.
- Dispute resolution and enforcement: Under this element, compliance with the CBPR System is enforced by the Accountability Agents and any other relevant Privacy Enforcement Authorities.

For more information on the CBPR System, please visit here.

Best Practices

Below is a list of recommended best practices relating to data protection for any organization operating in the United States. As the laws and regulations are constantly changing, we recommend you keep abreast of any changes in the law and continually reassess your compliance with data privacy and security regulations. This list is not exhaustive.

1. Provide a data privacy policy to customers, clients and donors and update it at least annually. If you have a website, the privacy policy should be placed clearly and conspicuously on your website.
2. Once a data privacy policy in place, ensure that your organization's staff are properly trained and prepared to follow the policy. Check regularly that employees do in fact comply with this policy.
3. Do not collect or retain personal information on customers or employees unless absolutely necessary.

4. Minimize gathering and using sensitive information from individuals, such as social security numbers or financial accounts information.
5. Train staff to regularly show that privacy protection is a priority and to ensure that information remains secure.
6. Consider appointing data protection officers to keep ahead of changes in the law and ensure that your organization remains up to date and compliant.
7. Regularly update and review data privacy and protection policies. If no policies are currently in place, assess privacy law obligations and develop internal and consumer facing policies consistent with US and international law.
8. Structure and enforce external agreements to ensure that any data transferred or shared between entities remains protected.
9. Dispose of any documents that contain personal information safely and security (i.e. with a shredder).
10. A privacy audit can help determine what kinds of personal information it collects, from whom, how it is collected, used, and stored, and the organization's ability to disclose it.