



# Legal, Regulatory, and Compliance Implementation on Security Controls

By: Mishelly Sandoval and Lucas Higgs


# The Family Educational Rights and Privacy Act (FERPA)

- The Family Educational Rights and Privacy Act is a federal law in the United States that protects the privacy of student education records. It applies to all educational institutions that receive federal funding, which includes schools and colleges. This federal law also gives certain rights to parents or eligible students (who are a minimum 18 years of age or attending a postsecondary institution). This federal law was enacted in 1974 and also applies to any education agency that receives funds under a suitable program of the US Department of Education.
- Main purpose:
  - Is to control access to and disclosure of student records. Schools must obtain written consent from a parent or an eligible student under this federal law before releasing any information from the student's educational records like the student's name, address, social security number, grades, attendance records, and other similar information.

# Family Educational Rights and Privacy Act

- **Key Components:**

- Data security- being able to establish protection measures for student records, training employees in data security practices and incident response.
- Monitoring and Auditing- Implementation of regular monitoring and auditing such as having internal audits periodically and data security assessments.
- Training and Education

- The Family Educational Rights and Privacy Act is not designed for non profit organizations specifically but there are still some benefits. Compliance with FERPA does encourage non profits to implement security measures for the protection of student education records. This helps to protect the privacy of the students and also helps to protect the organization against data breaches and unauthorized access.
- 

# Children's Online Privacy Protection Act (COPPA)

- Children's Online Privacy Protection Act (COPPA) is a law that requires the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The primary goal of COPPA is to place parents in control over what information is collected from their young children (under 13) online. The information could be collected from operators of commercial websites and online services as well as general audience websites. (Vedova, 2023)
- Why is it applicable to TKH?
  - TKH is a nonprofit so it's under the category of those not subjected to COPPA but it would be encouraged to post privacy policies online and protect COPPA's protections to potential child visitors. TKH's website is not directed towards children under 13, both fellowships offered require students to be older than 13 so they would also not be knowingly collecting, using or disclosing personal information from children within that age group.

# COPPA continued

- Does TKH's current secure program satisfy this legal or regulatory requirement? Yes or No and Why?
  - TKH is technically not subjected to COPPA but it does have privacy policies when the user initially opens the page, therefore it does satisfy the legal requirement
- What are the fines for violating this law or regulation?
  - A court can hold operators who violate the Rule liable for civil penalties of up to \$50.120 per violation. COPPA gives states and certain federal agencies authority to enforce compliance with respect to entities over which they have jurisdiction ( "History of COPPA Violations", n.d.)


# Stop Hacks and Improve Electronic Data Security (SHIELD Act)

- Is a law in New York that strengthens their data security laws by: (1) expanding the types of private information for which companies must provide customer notice in event of a breach and (2) requiring that companies develop, implement, maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information (“SHIELD Act”, n.d.)
- Why is it applicable to TKH?
  - TKH’s main office is house in New York (the Bronx specifically) so they must abide by this act
- What are the fines for violating this law or regulation?
  - For failure to provide timely notification, the court may impose a civil penalty of up to \$20 per instance of failed notification, not to exceed \$250,000. For failure to maintain reasonable safeguards, the court may impose a civil penalty of up to \$5,000 per violation (“SHIELD Act”, n.d.)

# Gramm-Leach-Bliley Act (GLBA)

- The Gramm-Leach-Bliley Act (GLB Act or GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways financial institutions deal with the private information of individuals. The Act consists of three sections:
  - **The Financial Privacy Rule**, which regulates the collection and disclosure of private financial information;
  - the **Safeguards Rule**, which stipulates that financial institutions must implement security programs to protect such information; and the
  - **Pretexting provisions**, which prohibit the practice of pretexting or accessing private information using false pretenses.
    - The Act also requires financial institutions to give customers written privacy policy notices that explain their information-sharing practices.

# Gramm-Leach-Bliley Act (GLBA)

- Purpose:
    - The standards established by GLBA complement data security requirements imposed by the Federal Deposit Insurance Corporation (FDIC). The purpose of the GLB Act is to ensure that financial institutions and their affiliates safeguard the confidentiality of personally identifiable information (PII) gathered from customer records in paper, electronic or other forms. The law requires affected companies to comply with strict data security guidelines. (Kranz, 2021)
    - GLBA compliance requires that companies develop privacy practices and policies that detail how they collect, sell, share and otherwise reuse consumer information. Consumers also must be given the option to decide which information, if any, a company is permitted to disclose or retain for future use. (Kranz, 2021)
    - GLBA's PII guidelines apply to any non-public personal information, which is defined as information a customer may provide to facilitate a transaction or which is otherwise obtained by the institution. (Kranz, 2021)
- 




# GLBA: Pretexting and Financial Privacy Rule

## Pretexting Rule:

- This rule aims to prevent employees or business partners from collecting customer information under false pretenses, such as social engineering techniques. Although GLBA does not have specific requirements regarding pretexting, prevention usually entails building employee training to avoid pretexting scenarios in the written information security document. (Kranz, 2021)

## Financial Privacy Rule:

- This rule, often referred to as the *Privacy Rule*, places requirements on how organizations may collect and disclose private financial data. An organization must give "clear and conspicuous notice" of its privacy policy at the start of a customer relationship. Subsequently, customers must get an annual notice for the duration of the relationship unless the organization meets certain criteria. (Kranz, 2021)
  - The Privacy Rule outlines which data will be collected, how it will be used and shared, who has access to it, and the policies and procedures used to protect it. As required by the Fair Credit Reporting Act, customers are to be notified of the privacy policy annually, including the right to opt out of sharing information with unaffiliated third-party entities. If a customer agrees to share information, the organization must abide by the provisions of the original privacy notice. (Kranz, 2021)
- 

# Safeguard Standard

- **Safeguard Rules: (Federal Student Aid)**

The objectives of the GLBA standards for safeguarding information are to –

- Ensure the security and confidentiality of student information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student (16 C.F.R. 314.3(b))

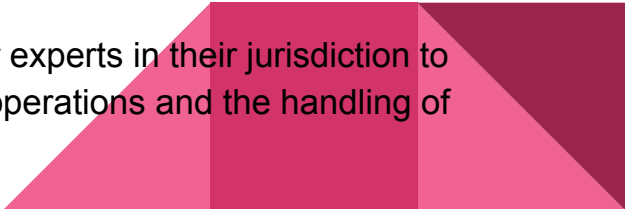
- **The rule instructs organizations to implement administrative, physical and technical protections as safeguards against cyber attacks, email spoofing, phishing schemes and similar cybersecurity risks.**
- The rule also requires an organization to designate at least one person to be accountable for all aspects of the information security plan, including development and regular testing. Data encryption and key management are recommended as best practices, but they are not FTC requirements under the Safeguard Rule.

# GLBA continued

- Penalties and Cases: (Kranz, 2021)

- Failure to comply with GLBA can have severe financial and personal consequences for executives and employees. A financial institution faces a fine up to \$100,000 for each violation. Its officers and directors can be fined up to \$10,000, imprisoned for five years or both. Companies also face increased exposure and a loss of customer confidence.
- Heightened awareness of security risks is among the benefits companies may derive from GLBA compliance, especially as hackers develop more sophisticated tools to breach computer systems. Aside from enhanced brand reputation, a company can gain new insights from existing data and improve its data management capabilities.
- Recent GLBA cases brought by the FTC include:
  - **Ascension Data and Analytics.** In 2020, the Arlington, Texas, company agreed to an undisclosed financial settlement after a vendor, OpticsML, was found to have stored customer financial information in plain text in insecure cloud storage.
  - **PayPal.** The online payment processor agreed to pay \$175,000 to the state of Texas in 2018 to settle GLBA and Federal Trade Act violations that compromised data security and privacy of customers using its Venmo peer-to-peer application.
  - **TaxSlayer.** Hackers were able to access nearly 9,000 of the Augusta, Ga., online tax preparer's customer records for several months in 2015. The FTC said it failed to implement a comprehensive security program, including providing a privacy notice to customers, as required under GLBA. Under the settlement with the FTC, the company is prohibited from violating the GLBA's Privacy Rule and the Safeguards Rule for 20 years and is required to have a third party assess its compliance every two years for 10 years.

# GLBA And How it relates to TKH

- The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, primarily applies to financial institutions and their handling of consumer financial information. As a result, its direct impact on non-profit organizations may be limited, as they typically do not fall under the definition of financial institutions.
  - However, it's important to note that non-profit organizations may still collect and handle personal information from their donors, supporters, and beneficiaries. In such cases, they may have obligations under other data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union or other applicable local regulations.
  - While the GLBA itself may not directly apply to non-profit organizations, they should still take measures to protect the privacy and security of the personal information they handle. This includes implementing appropriate data protection practices, maintaining confidentiality, obtaining consent where required, and ensuring compliance with applicable data protection laws.
  - It's advisable for non-profit organizations to consult legal professionals or experts in their jurisdiction to understand the specific requirements and regulations that apply to their operations and the handling of personal information.
- 

# GLBA and GDPR


- GLBA and Europe's General Data Protection Regulation (GDPR) have different goals, but both define data security and consumer privacy. Whereas GLBA sets data privacy rules for financial institutions, GDPR encompasses any organization that processes an individual's personal data in the course of transacting business. (Kranz, 2021)
- Like GLBA, GDPR encourages companies to be more transparent in how they capture and handle sensitive information. That includes individuals' personal data and any metadata that may be used to identify or characterize them. (Kranz, 2021)



# General Data Protection Regulation

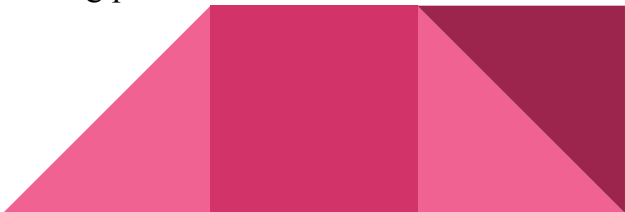
The General Data Protection Regulation (GDPR) is a comprehensive data protection law that came into effect in the European Union (EU) on May 25, 2018. It has had a significant impact on both the educational and business sectors.

## **Educational Sector:**

- **Consent and Privacy Notices:** Educational institutions must obtain explicit and informed consent from individuals for collecting and processing their data and provide privacy notices outlining the purpose, legal basis, and retention period of data processing.
  - **Data Protection Officer (DPO):** Some educational institutions may need to appoint a DPO to ensure GDPR compliance and act as a point of contact for individuals and supervisory authorities.
  - **Security and Confidentiality:** Schools and universities must implement security measures to protect personal data from unauthorized access, loss, or disclosure.
  - **Data Subject Rights:** Individuals have various rights, such as access, rectification, erasure, and objection to data processing, which educational institutions must address.
  - **Data Transfers:** Adequate safeguards must be in place when transferring personal data outside the EU.
- 

# GDPR: Business Sector

## **Business Sector:**

- Lawful Basis for Processing: Businesses must establish a legal basis for processing personal data, such as contractual necessity or legitimate interests.
  - Data Subject Rights: Individuals have rights regarding their data, and businesses must respect and address these rights.
  - Data Protection Officer (DPO): Some businesses may need to appoint a DPO to oversee GDPR compliance and serve as a point of contact.
  - Privacy by Design and Default: Privacy measures should be integrated into What are the consequences of non-compliance with GDPR? Products and services from the early stages of development.
  - Data Breach Notifications: Businesses must notify authorities and individuals in case of data breaches that pose risks to individuals' rights and freedoms.
  - International Data Transfers: Adequate safeguards are required when transferring personal data outside the EU.
- 


# GDPR Summary

- The GDPR introduced comprehensive data protection regulations in the EU. Compliance with the GDPR is crucial to protect personal data, avoid fines, and maintain a positive reputation. In the educational sector, institutions must obtain consent, ensure security, respect individuals' rights, and establish procedures for data transfers. Similarly, businesses must develop lawful bases, respect individuals' rights, appoint DPOs if necessary, implement privacy measures, handle data breaches, and ensure adequate safeguards for international data transfers.





# The Payment Card Industry Data Security Standard (PCI DSS)

- Is a set of security standards established by major credit card companies, including Visa, Mastercard, American Express, Discover, and JCB. Its purpose is to ensure the secure handling of payment card information and protect cardholder data from theft, fraud, and unauthorized access.
  - The PCI DSS provides a comprehensive framework of requirements and best practices that organizations must adhere to if they handle, process, store, or transmit payment card data. It applies to various entities, including merchants, service providers, financial institutions, and any organization that accepts payment cards.
  - The PCI DSS comprises twelve high-level requirements, further broken down into specific sub-requirements. These requirements cover various aspects of data security, including network security, system configurations, access controls, encryption, monitoring, and regular testing. Some of the essential requirements include:
    - We install and maintain secure network infrastructure, including firewalls and closed configurations.
    - They protect cardholder data through encryption and secure storage.
    - We are implementing strong access control measures, including unique user IDs, strong passwords, and restrictions on physical access.
    - We are regularly monitoring and testing networks and systems for vulnerabilities.
- 


# PCI DSS Regulatory Requirements

- Organizations that handle payment card data must achieve and maintain compliance with the PCI DSS. Compliance can involve self-assessment questionnaires, external audits by Qualified Security Assessors (QSAs), and regular reporting to payment card brands. Compliance requirements may vary based on factors such as the volume of card transactions and the organization's role in the payment card ecosystem.
- By complying with the PCI DSS, organizations demonstrate their commitment to protecting sensitive cardholder data and reducing the risk of data breaches. Compliance helps maintain customer trust, avoids financial penalties, and ensures a secure payment card environment.
- How can a specific program satisfy the regulatory requirements of the PCI DSS?
  - To satisfy the regulatory requirements of the Payment Card Industry Data Security Standard (PCI DSS), a specific program should focus on the following key steps:
  - Scope identification: Define the cardholder data environment (CDE) and identify systems, processes, and people that handle or have access to cardholder data.
  - Compliance assessment: Conduct a thorough evaluation to identify gaps and vulnerabilities in security controls and processes.
  - Data encryption: Encrypt cardholder data during transmission and storage using robust encryption algorithms and critical management practices.
  - Secure network infrastructure: Implement strong network security controls, such as firewalls, network segmentation, and intrusion detection/prevention systems.

# PCI DSS: Satisfying Regulatory Requirement

- How can a specific program satisfy the regulatory requirements of the PCI DSS?
  - Access controls: Limit access to cardholder data on a need-to-know basis using unique user IDs, strong passwords, and two-factor authentication.
  - Vulnerability management: Regularly scan and test systems for vulnerabilities, patch and update promptly, and establish a patch management program.
  - Secure coding practices: Implement best coding guidelines and rules for software applications handling cardholder data.
  - Logging and monitoring: Implement robust logging and monitoring mechanisms to detect and respond to security incidents.
  - Incident response: Develop and maintain an incident response plan and regularly test and update it as needed.
  - Employee awareness and training: Provide regular security awareness and training programs to promote a security-conscious culture.
  - Auditing and compliance reporting: Conduct regular internal audits and engage a Qualified Security Assessor (QSA) if required. Prepare and submit compliance reports to payment card brands.
  - Maintaining compliance with PCI DSS is an ongoing process that requires regular reviews, assessments, and updates to security controls to adapt to the evolving security landscape and protect cardholder data.

# PCI DSS Violation Examples

- In what ways can a medium non-profit violate the PCI DSS? (Examples )
    - We store sensitive cardholder data beyond what is necessary instead of tokenization or encryption.
    - Allowing weak passwords or using default vendor-supplied passwords rather than enforcing strong password policies and multi-factor authentication.
    - They fail to implement robust network security measures like firewalls, intrusion detection/prevention systems, and regular vulnerability scanning.
    - Not restricting access to cardholder data on a need-to-know basis, including inadequate user access management and role-based access controls.
    - You must provide sufficient security awareness and training programs to staff, leading to a lack of understanding and compliance.
    - They must ensure that third-party service providers handling cardholder data are PCI DSS compliant.
    - These violations can result in potential penalties, reputational damage, and an increased risk of data breaches for the non-profit organization. Nonprofits must understand and address these areas to maintain PCI DSS compliance and protect cardholder data.
- 

# PCI DSS Violation Consequences

- What are the fines/consequences associated with violating the PCI DSS?
  - Fines from Payment Card Brands: Payment card brands, such as Visa, Mastercard, American Express, Discover, and JCB, can impose penalties on non-compliant organizations. The penalties can vary depending on the severity and duration of the non-compliance.
  - Increased Transaction Fees: Non-compliant organizations may face higher transaction fees imposed by payment card brands due to their failure to meet PCI DSS requirements.
  - Reputational Damage: Non-compliance with PCI DSS can lead to reputational damage for organizations. News of a data breach or non-compliance can erode customer trust and confidence, resulting in potential loss of business and damage to the organization's reputation.
  - Legal Consequences: Non-compliance may also result in legal consequences, such as lawsuits from affected individuals, regulatory investigations, and potential fines or penalties imposed by government authorities or regulatory bodies.
  - Loss of Card Processing Privileges: In severe non-compliance or repeated violations, payment card brands may revoke an organization's privilege to process payment card transactions. This can substantially impact the organization's ability to conduct business.
  - Remediation Costs: Organizations found to be non-compliant will incur costs to address the identified issues, implement necessary security measures, and achieve compliance. These costs include technology investments, audits, assessments, and remediation efforts.
  - It is important to note that the specific fines and consequences associated with PCI DSS violations may vary based on the circumstances, the level of non-compliance, and the response of the payment card brands and regulatory authorities involved. Organizations should prioritize PCI DSS compliance to avoid these penalties and protect their reputation, customer trust, and financial stability.