EzeCastle INTEGRATION

Privacy Compliance Consulting

High-profile data and security breaches are resulting in new regulations that impact the way all firms conduct business.

Building on the federal Gramm-Leach-Bliley Act, local state governments are instituting stricter regulations to protect personal information. The Massachusetts state law 201 CMR 17 is just one example of the changing regulatory landscape.

MA 201 CMR 17 requires any company that owns, licenses, stores or maintains personal information about a Massachusetts resident to develop, implement and maintain a comprehensive, written information security program (WISP). The regulation also outlines required computer system security safeguards firms must have in place.

Eze Castle Integration's Eze Privacy Compliance Consulting services help firms navigate the new regulations and take the necessary actions to help ensure compliance. Eze Castle consultants use the following proven methodology to develop and implement a comprehensive information security program for firms:

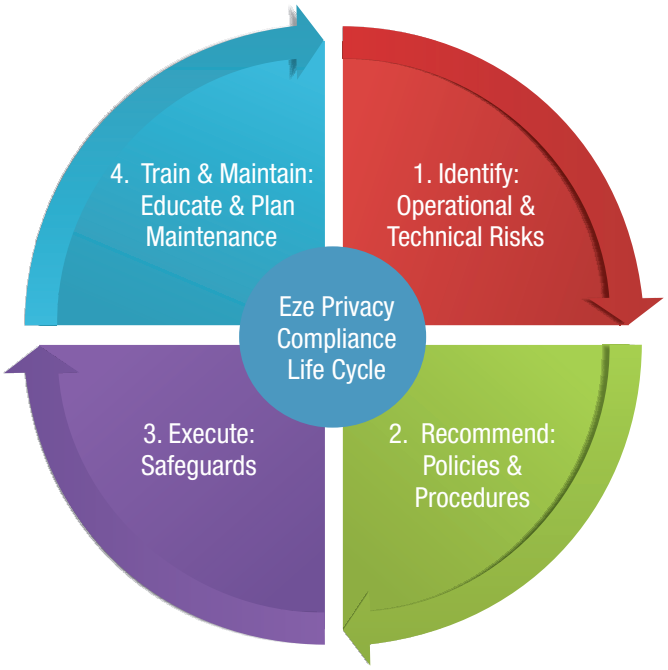
- Identify Operational & Technical Risks
- Recommend Policies & Procedures
- Execute Safeguards
- Train & Maintain Program

Operational & Technical Risks

Eze Castle begins by conducting a comprehensive operational and technical assessment focused on identifying where investor and employee personal information, both electronic and hard copy, resides and the safeguards in place to protect it.

Assessment activities include:

- Determining what personal information exists, who has access and where it resides
- Identifying existing software and hardware, and evaluating associated security schemes
- Verifying third-party compliance



About Eze Castle Integration

Eze Castle Integration (www.eci.com) is the leading provider of technology, IT services and consulting to the investment industry. The company's service areas include Startup and Relocation, Outsourced Technology Support, Professional Services, Telecommunications, Disaster Recovery and Business Continuity Planning, Archiving, Storage, and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in Chicago, London, Los Angeles, Minneapolis, New York, San Francisco, and Stamford.

Policies & Procedures

Once the assessments are complete and the personal information is located, Eze Castle determines the administrative, physical and technical safeguards required to protect the personal information maintained, utilized and accessed at the company.

Eze Castle will define the recommended policies and procedures necessary to ensure the company is compliant with regulatory requirements.

Execute Safeguards

The next phase is a twofold process that involves implementing the Technical Solution(s) and Administrative Programs needed to safeguard the company's infrastructure and personal information.

Technology safeguards may include access control, encryption software and firewall protection. The need for technical enhancements will depend on what a company already has in place.

Administrative safeguards center on the development of a written information security program (WISP) that will outline a company's policies and procedures for protecting personal information. The WISP will identify roles and responsibilities for handling personal information.

This will include a company's physical methods of accessing, collecting, storing, using, transmitting and destroying personal information. The WISP will also provide procedures for responding to a violation of the WISP or a data breach.

Train & Maintain

Employee training and program maintenance are key to staying compliant and avoiding data breaches. Eze Castle provides training to ensure all employees know the procedures for handling personal information and the consequences if personal information is compromised.

Eze Castle also offers an annual maintenance program to ensure the WISP is kept current and always reflects company changes.

PERSONAL INFORMATION DEFINED

According to Massachusetts law, personal information is an investor's or employee's first and last name or first initial and last name with one or more of the following data elements:

- Social Security Number (or their equivalent issued by governmental entities outside the United States)
- Taxpayer Identification Numbers (or their equivalent issued by governmental revenue entities outside the United States)
- Employer Identification Numbers (or their equivalent issued by government entities outside the United States)
- State or foreign drivers license numbers
- Date of birth
- Financial account number or credit/debit card number

MORE INFORMATION

Eze Privacy Compliance helps firms navigate the evolving regulatory landscape and take the necessary actions to achieve compliance.

To learn more,
Call today: 800.752.1382
or Visit our website at www.eci.com