CERTIFIED DATA PRIVACY PRACTITIONER (CDPP) TRAINING

A 16 Hours Certified Data Privacy Training

America | Canada | Europe

Dates : November 2nd – 5th ,2020
Time : 9.00 AM to 1.00 PM ET
Mode : Online

Course Fees:
Non-ISACA Members: USD $120 ISACA Members: USD $100

INTRODUCTION

Recent history has seen drastic changes in the way personal data is being collected and handled by businesses. The dependence on data to drive routine businesses and utilizing it for innovation have raised potential threats and risks to the privacy of individuals. Data privacy is the right of an individual to control how personal information is collected, with whom it is shared, and how it is processed, retained, or deleted. Better understanding the laws of privacy and data protection will enable you to protect your organization and safeguard the customers' personal information.

IMPORTANCE OF DATA PRIVACY

The way technology is advancing, and the way data collection is becoming more and more sophisticated (with or without knowledge of the consumer), it is important for individuals to have some control over their personally identifiable information (PII) and personal health information (PHI) i.e. what needs to be disclosed/ not to be disclosed, where PII & PHI should be used (purpose) etc. As a result, data privacy has emerged as one of the most significant aspects of today's world. Apart from regulatory requirements, protecting the privacy of data reduces the risk of costly incidents and reputational harms as well.

WHY DATA PRIVACY ?

Data privacy is the right of an individual to have control over what personal information can be collected and how is it used. Many consider data privacy to be the most significant consumer protection issue today. The risk of PII being exposed to an unauthorized personnel has increased many folds and high-profile data breaches have created heightened concern about how data may be protected and kept private. Compliance requirements for data privacy are getting more complex as different jurisdictions enact their data protection laws.

WHAT IS CDPP ?

In line with the rising concerns on data privacy, we have drafted a 4-day online workshop – Certified Data Privacy Practitioner (CDPP). We will discuss real-world, practical approaches to how professionals can navigate the complex landscape of privacy requirements to best protect their organizations and comply against the local & global data protection laws.

OBJECTIVE OF CDPP PROGRAM

- Overview of privacy and data protection for the global organization
- Provide methods for protecting privacy using the Fair Information Principles
- Identify local and global laws and regulations that pertain to data protection
- Identify strategies for managing compliance issues related different privacy laws and data protection acts
- Implementing data security in practice
- A useful privacy framework

REGULATIONS TO BE COVERED

- EU's General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- ISO 27701: The International Standard for Data Privacy
- COPPA - Children's Online Privacy Protection Act
- The California Online Privacy Protection Act (CalOPPA)
- California Consumer Privacy Act (CCPA)
- GLBA - Gramm-Leach-Bliley Act, USA
- The Personal Information Protection and Electronic Documents Act (PIPEDA), Canada
- The Privacy Deregulation Act 2018, Austria
- DIFC, Data Protection Law 2020 – Dubai
- Data Privacy Act of 2012, Philippines
- Privacy Act 1988, Australia

REGULATIONS TO BE COVERED

The General Data Protection Regulation (GDPR)

GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Data controllers must clearly disclose any data collection, declare the lawful basis and purpose for data processing, and state how long data is being retained and if it is being shared with any third parties or outside of the EEA. It is based on principles of consent, transparency, protection, and user control.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA establishes a set of national standards for the use and disclosure of an individual's health information – called protected health information – by covered entities, as well as standards for providing individuals with privacy rights to understand and control how their health information is used. It was created primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage

COPPA - Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA) took a first step at regulating personal information collected from minors. The law specifically prohibits online companies from asking for PII from children 12-and-under unless there's verifiable parental consent. The personal information to be protected, including screen names, email addresses, video chat names, as well as photographs, audio files, and street-level geo coordinates. The originating website operator must take "reasonable steps to release children's personal information only to companies that are capable of keeping it secure and confidential." Fines for failing to comply with the law were recently increased to up to $43,280 per privacy violation per child.

The California Online Privacy Protection Act (CalOPPA)

In 2004, CalOPPA was drafted to protect the privacy rights and personal data of California residents**.** It requires websites to post privacy policies detailing data collection and use. The operators of commercial websites that collect Personally Identifiable Information (PII) from California's residents are required to conspicuously post and comply with a privacy policy that meets specific requirements. A website operator who fails to post their privacy policy within 30 days after being notified about non-compliance, will be deemed in violation of CalOPPA by government officials seeking civil penalties or equitable relief, or by private parties seeking private claims.

California Consumer Privacy Act (CCPA)

Officially in effect from January 1, 2020, the CCPA boasts three guiding principles; transparency, accountability and control. It demands that companies inform users of data processing, take extra measures to protect user information and allow users a say in what data is collected and how it is shared. Under the CCPA, California residents ("consumers") are empowered with the right to opt out of having their data sold to third parties, the right to request disclosure of data already collected, and the right to request deletion of data collected.

GLBA - Gramm-Leach-Bliley Act, USA

Gramm-Leach-Bliley Act (GLBA) is an enormous slab of banking and financial law that has buried in it important data privacy and security requirements. It Protects non-public personal information (NPI), which is defined as any "information collected about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available" — essentially PII with an exception for any widely available financial information — for example, property records or certain mortgage information. Penalties for non-compliance can include fines of up to $100,000 per violation, with fines for officers and directors of up to $10,000 per violation. The provisions also include criminal penalties of up to five years in prison, and the revocation of licenses.

REGULATIONS TO BE COVERED

ISO 27701: The International Standard for Data Privacy

ISO 27701 provides specific requirements and guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) as an extension of the flexible Information Security Management System (ISMS) defined in ISO 27001. Compliance with ISO 27701 first requires compliance with the requirements of ISO 27001. They are intended to complement each other. The ISO 27701 is developed to provide guidance on what measures should be taken to ensure the privacy of any personal data that the organizations process while meeting the best practices outlined in GDPR and other data privacy laws worldwide.

The Personal Information Protection and Electronic Documents Act (PIPEDA), Canada

PIPEDA was introduced on April 13, 2000 to promote consumer trust in electronic commerce. It mandates that businesses using data for, or in the course of commercial activities, must disclose the purpose of that data collection to the owners of that data, and obtain consent to proceed. Any private enterprise in Canada that collects personal information during the course of commercial activity is subject to PIPEDA.

The Privacy Deregulation Act 2018, Austria

The 'Data Protection Act' (Datenschutzgesetz, DSG) has considerably amended the Data Protection Act 2000. In addition to the GDPR, it is now the central piece of legislation in Austria regulating data privacy. The DSG, as amended by the Privacy Deregulation Act 2018, came into force on May 25, 2018 and is now the applicable regulation in Austria. The DSG applies to processing of personal data in Austria, as well as processing of personal data in any EU Member State, if such processing occurs for the purpose of an Austrian-based main establishment or a branch office of a data controller. All employees, agents or contractors of a controller or a processor must be subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

DIFC, Data Protection Law 2020 – Dubai

On July 1, 2020, the Dubai International Financial Centre (“DIFC”) Data Protection Law No. 5 of 2020 came into effect and is set to be enforced from 1 October 2020. The New DP Law replaces DIFC Law No. 1 of 2007. The goal is to establish enhanced governance and transparency requirements that will place DIFC on par with international laws and regulations. The New DP Law reflects many aspects of the EU’s General Data Protection Regulation (the “GDPR”). The New DP Law also incorporates certain aspects of the California Consumer Privacy Act of 2018 (“CCPA”) and its proposed regulations. Breach notifications are now required as per the DIFC Law and the new law sets a maximum fine of USD 100,000 for administrative breaches, with additional scope for larger fines (unlimited) for more serious violations.

Data Privacy Act of 2012, Philippines

Based in the Philippines, but applicable to all the businesses that process the data of Philippines citizens and residents. The Data Privacy Act of 2012 is centered on the principle that data processing should be transparent, proportional and based on legitimate purposes. The law requires government and private organizations composed of at least 250 employees or those which have access to the personal and identifiable information of at least 1000 people needs to appoint a Data Protection Officer.

The Privacy Act 1988, Australia

It establishes information privacy principles for Australian citizens when it comes to the collection of their data by government, organizations, companies contracted to work with government organizations and health service providers. Information can only be collected if it is relevant to the agencies' functions. Upon this collection, that law mandates that Australians have the right to know why information about them is being acquired and who will see the information.

COURSE CONTENT

Part 1:

- Introduction to GDPR
- Principles of GDPR and data subject rights
- Concept of data protection impact assessment
- Liabilities and penalties of GDPR
- Introduction to HIPAA
- Identification of the standardized code sets as mandated by HIPAA
- Liabilities and penalties of HIPAA
- Introduction to US Federal Laws - COPPA, CALOPPA, CCPA, GLBA
- Terms and definitions of the different US Federal data protection law.
- Applicability and jurisdiction of COPPA, CALOPPA, CCPA, GLBA
- Liabilities and penalties of COPPA, CALOPPA, CCPA, GLBA
- Principles of COPPA, CALOPPA, CCPA, GLBA and data subject rights.
- Introduction to PIPEDA
- Terms and definitions of PIPEDA.
- Applicability and jurisdiction of Canadian data protection law
- Liabilities and penalties of PIPEDA

Part 2

- Overview of ISO 27701: The International Standard for Data Privacy
- Introduction to the Privacy Deregulation Act 2018, Austria
- Introduction to DIFC, Data Protection Law 2020 – Dubai
- Introduction to the Data Privacy Act of 2012, Philippines
- Introduction to the privacy Act 1988 – Australia
- Terms and definitions of the local data protection laws.
- Applicability and jurisdiction of the local data protection laws
- Principles of local data protection laws.
- Liabilities and penalties of local data protection laws.

Part 3

- Data protection Implementation guidelines
- Identifying PII and PHI in your organization
- Inventorying PII and PHI and assigning ownership
- Developing security controls to ensure compliance with local data protection laws, GDPR, and HIPAA
- GDPR Privacy Impact Assessment

Part 4

- Appointing a Data Privacy Officer(DPO)
- Roles and responsivities of the DPO
- Developing appropriate policies and procedures
- Board and senior management oversight on the privacy program
- Measuring success of your privacy program

Part 5

- How does local privacy laws co-relate with GDPR and HIPAA
- Key pointers to implementing compliances successfully
- Key Challenges in DPA/GDPR & HIPAA implementations

Examination – The participants would need to undergo an online examination after the training. On successfully clearing the examination, the participant would be awarded with the CDPP certificate.

“Remember….. you are the Centre of Security”

Udit Pathak,
Practice Lead - Cloud Security,
Network Intelligence

Udit Pathak brings in 10+ years of experience working in the payment security space. He currently leads Cloud Security practices at Network intelligence, focusing on security review of cloud, configuration review, cloud governance framework development, Vulnerability assessment (IT infrastructure and various components) and technical security audits, on Information Security audits (ISO, GDPR, HIPAA & PCI DSS). His hands-on experience working in the cyber security domain helps his audience connect to the real-life scenarios and understand the practical applications of the Data Privacy laws.

Registration form: https://bit.ly/2SQ5sHI