NETWORK INTELLIGENCE
Global cybersecurity provider

CERTIFIED DATA PRIVACY PRACTITIONER (CDPP) TRAINING

A 16 hours certified data privacy training

Americas | Europe

Dates : 10th-13th August, 2020
Time : 2.00 PM to 6.00 PM (GMT + 1)
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)
- The Privacy Deregulation Act 2018, Austria
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- California Consumer Privacy Act (CCPA)
- The California Online Privacy Protection Act (CalOPPA)
- The personal Information Protection and Electronic Documents Act, Canada (PIPEDA)
- Bundesdatenschutzgesetz, Germany (BDSG),
- Personal Data Protection Bill 2018, India
- Data Privacy Act of 2012, Philippines
- Privacy Act 1988, Australia

REGULATIONS TO BE COVERED

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.

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.

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.

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.

BDSG **Bundesdatenschutzgesetz** (**BDSG**), Germany

Widely accepted as the earliest data protection law, the BDSG sets rigid standards under which businesses are required to adopt and maintain protective measures for data storage in IT systems. BDGS governs the exposure of personal data, which are manually processed or stored in IT systems. The collection, processing and use of personal data is strictly prohibited, unless it is permitted by the law or the person concerned gives consent. If data is permitted to be collected for a particular purpose, use of the data is restricted to this purpose

Personal Data Protection Bill 2018, India

The bill seeks to provide protection of personal data of individuals, and establishes a Data Protection Authority for the same. The legislation sets privacy and data protection standards and notably introduces mandatory annual data audits. The offences under the bill include: (i) processing or transferring personal data in violation of the bill is punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher, and (ii) failure to conduct a data audit is punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary, whichever is higher.

REGULATIONS TO BE COVERED

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 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.

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

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 The California Online Privacy Protection Act (CalOPPA)
- Terms and definitions of data protection law.
- Applicability and jurisdiction of CalOPPA
- Liabilities and penalties of CalOPPA
- Introduction to California Consumer Privacy Act (CCPA)
- Principles of CCPA and data subject rights.
- Applicability and jurisdiction of CCPA
- Liabilities and penalties of CCPA
- Introduction to PIPEDA
- Terms and definitions of PIPEDA.
- Applicability and jurisdiction of Canadian data protection law
- Liabilities and penalties of PIPEDA

Part 2

- Introduction to Bundesdatenschutzgesetz (BDSG), Germany
- Introduction to the Personal Data Protection Bill 2018, India
- Introduction to the Data Privacy Act of 2012, Philippines
- Introduction to the privacy Act 1988 – Australia
- Introduction to the Privacy Deregulation Act 2018, Austria
- 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, PCI DSS and HIPAA

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”

OUR TRAINER

KK Mookhey
CEO and Founder of Network Intelligence
CISA, CISM, CRISC, CISSP, PCI QSA, ACFE

KK is one of the pioneers in the cybersecurity domain. Having begun Network Intelligence as a one-man show in 2001, it has grown to a team of over 700 consultants spread across offices in New York, Dubai, Mumbai and Singapore. He is a trusted consultant and trainer to organizations across the globe on various aspects of cybersecurity. He is well-versed with the security challenges of various industry verticals and with international standards and frameworks such as ISO 27001, PCI DSS, COBIT, HIPAA, GDPR. He is the author of two books (on Linux security and on the Metasploit framework) and of numerous articles on Information security. He was the first security researcher from India to present at Blackhat 2004 (on Detection and Evasion of Web Application Attacks) and has spoken at numerous global conferences. He is currently overseeing the research activities at Network Intelligence on use of big data in security, building various automation solutions, and security impact of Internet of Things.

Registration form: https://bit.ly/2Z3cGdR