27 Pine Street, Suite 700
New Canaan, CT 06840
Phone: (203) 972-3567 Fax: (203) 972-3367
e-mail: Levinemh@auditserve.com Website: http://www.auditserve.com

IT Audit Seminars

GDPR Implementation, Assessment, and Auditing Approaches

Background

With the passing of General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) in which all companies who have past & present EU resident's data, will be required to implement business processes and technical solutions to meet the GDPR mandates which includes complete removal of all traces of an individual' identify from the company's systems if requested. Companies will need to comply or be subject of fines of 4% of annual revenues by the Supervisory Authority. Individual data subjects also have the right to compensation from Controllers and Processors (Article 82) for instances in which their rights are violated as defined within. This regulation not only impacts EU companies but all companies worldwide whose customers and employees reside in the EU. GDPR requires Controllers to only utilize Processors which are GDPR compliant (Article 28). In addition, since Processors are equally liable as Controllers this is the first time in history that Processors will be performing due diligence reviews of their clients (who are the Controllers) to ensure they are GDPR compliant.

Seminar Objective

This GDPR seminar has been restructured to provide attendees a consolidated view of how to implement, assess and audit the project . This seminar is intended to provide attendees the base level knowledge required to (1) conduct a "point-in-time" Assessment to provide a basis to determine the current stage of GDPR compliance and identify the remaining project initiatives, (2) manage the implementation of the GDPR project, and (3) conduct a GDPR Pre-Implementation Audit. Audit Serve has completed three GDPR Impact Analysis of organizations who are both Controllers and Processors and provides ongoing GDPR advisory services to these organizations. The experiences from these completed consulting projects along with its current GDPR project of performing all aspects of the GDPR Implementation for a multi-national Controller have been incorporated into this seminar.

Seminar Length

Two days (7 hour presentation time per day plus 1 hour lunch and four 10 minute breaks per day)

Who Should Attend

The seminar for mid-level IT (including GDPR project managers), GRC and audit professionals but would also be highly invaluable for Senior Management who need to understand the scope of this project and how it impacts their organizations

GDPR Implementation, Assessment, and Auditing Approaches

Continuing Professional Education Credits

All attendees are eligible to receive 15 hours of continuing professional education (CPE) credits by attending. These credits are recognized by the National Association of State Boards of Accountancy (NASBA). The CPE field of study is Accounting and Auditing. No prerequisites or advanced preparation is required. Audit Serve is registered with the National Association of State Boards of Accountancy (NASBA), as a sponsor of continuing professional education on the National Registry of CPE Sponsors.
State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding sponsors may be addressed to National Registry of CPE Sponsors, 150 Fourth Avenue North, Suite 700, Nashville, TN 37219-2417, USA (615) 880-4200 Web site: www.nasba.org.

Instructor & Organizer's Biography Mitchell H. Levine, CISA

Mitchell Levine, CISA is the founder of Audit Serve, Inc. which was established in 1990. For the last 26 years at Audit Serve, Mitch has split his time between traditional IT & Integrated Audit Consulting projects and global project initiatives. For the past 18 months Mitch has been focusing most of his time on the GDPR project in which he has presented his GDPR seminar four times in the last 9 months in which three of these presentations occurred in Europe. He has completed GDPR Impact Analysis & Assessment projects for three separate organizations and completed a long-term engagement for one large international organization mapping all of their business processes that utilize personal data and linking them to delivery packages that will be the basis for responding to Subject Access Rights (SAR) Requests that all organizations in-scope for GDPR will be requested to provide starting May 25, 2018.

Detailed Seminar Outline

I. Introduction to General Data Protection Regulation

Precursor to GDPR
What brought about GDPR?
What is compelling compliance?
Who is impacted?

- Overall basis
- Applying Article 3 Territorial Scope
- US-based companies
- Employers of employees residing in the EU
- UK situation

Key Players within GDPR
Terminology
High level introduction of key regulations
Structure of regulations

II. Performing a GDPR Pre-Implementation Review/Audits
Note: detailed discussion relating to each GDPR article occurs as part of section IV
Typical Pre-imp reviews
Audit alternatives for the GDPR project

III. Performing a GDPR Project Assessment
Note: detailed discussion relating to each GDPR article occurs as part of section IV
What is a project assessment?
Recommended approaches to conducting the GDPR Project Assessment
Establishing a scorecard for the GDPR Project Assessment

GDPR Implementation, Assessment, and Auditing Approaches

Detailed Seminar Outline (continued)

IV. Understanding the Regulations, Implementation Assessment and Audit Approaches

This section of the seminar which represents 65% of the seminar goes through each of the GDPR articles and (1) identifies the critical components of each Article, (2) Implementation Guidance for each of these key Articles, (3) Key Assessment questions to ask for each Article and the (4) Audit procedures based on performing a full scale pre-implementation review.

Key GDPR articles covered

- Record of Processing Activities (Article 30)
- Information Controllers which must be provided to Data Subject at time when personal data is obtained (Article 13)
- Information Controllers which must be provided to Data Subject where personal data have not been obtained from Data Subject (Article 14)
- Right to Access (Articles 15)
- Right to Recertification (Article 16)
- Transfers of personal data to third countries
  Cross Border Data Transfer/Safe Harbor (Article 44)
- Data Portability (Article 20)
- Expressed Consent (Article 7)
- Condition's applicable to Child's consent relation to information society services (Article 8)
- Processing of Special categories (Article 9)
- Right to Erasure/Right to be forgotten (Article 17)
- Processor (Article 28)
- Right to Object to Processing (Article 21)
- Lawfulness of Processing (Article 6)
- Security of Processing (Article 32)
- Data Breach Notification (Articles 33 and 34)
- Data Protection by Design and Default (Article 25)
- Data Protection Impact Assessment (Article 35)
- Processor Requirements (Article 28)
- Automated individual decision making/profiling (Article 22)
- Right to Restrict Processing (Article 18)
- Right to Object to Processing (Article 21)
- Recipients of personal data (Article 19)
- Lawfulness of Processing (Article 6)
- Condition's applicable to Child's consent (Article 8)
- Processing of Special categories (Article 9)

- US based considerations
- Understanding the role of the Data Protection Officer

Detailed Seminar Outline **(continued)**

V. Global Project Initiatives

- Understanding Data Relationships, business relationships and global data mapping requirements
- Designing & Processing Subject Access Requests (SARs)
- Identifying and managing third parties
- Business & IT Change Requirements
- GDPR Compliance Monitoring
- Other GDPR Initiatives/Activities

VI. Conducting the GDPR Audit

- Auditing the GDPR project impact analysis to define its business processes which are inscope for GDPR
- Evaluating the data repository has been established to meet the requirements of Article 30 Record of Processing which maps personal data to business processes and business justification for retaining data as required by Article 25
- Assessing whether customer data disclosure requirements and expressed consents have been established for inscope business processes
- Validating whether organization has established implemented initiatives to support Data Portability (Article 20), access to data (Article 15 & 16), and erasure of data and has established a system to support the processing of SARs.
- Validating whether processing components in which data subject can object to processing (Article 21) have been identified and integrated into the SAR process.
- Validating whether all processors used by the organization that are inscope for GDPR have been identified and their GDPR compliance has been validated
- For employees who are located in EU countries, determine whether a project initiative been established to meet the GDPR requirements for disclosure and processing of SAR Requests
- Evaluating whether Data Breach notification process which meets Article 32 & 33 requirements
- Determine whether organization established their interpretation of Article 32 Security of Processing and established a gap listing or final compliance specification