Take Away
1) Google GDPR? AIG Europe?
2) SAR (Subject Access Request)
3) Control is bidirectional (controller–processor) — must ensure that controller is GDPR
4) Cannot use non-GDPR compliant processor
5) GDPR is principle based

2018-04-11

Skills
- GDPR
- Data / Process

GDPR Assessment, Implementation and Auditing Approaches

Instructor: Mitchell Levine, CISA

AUDIT SERVE INC.

27 Pine Street Suite 700
New Canaan, CT 06840
Levinemh@auditserve.com www.auditserve.com
203-972-3567 Fax: 203-972-3367

April 11, 2018
Greater Hartford ISACA & Southern New England IIA Chapters

Audit Vision
Free monthly IT Audit & Security email Newsletter since 1991
Join 3,500 other free subscribers
www.auditserve.com

These seminar materials are to be used for your personal use only as a registered attendee of the ISACA & IIA Chapter's GDPR. GDPR Seminar and cannot be redistributed to anyone else or posted on any website or in the cloud. No software is to be used create a non-password protected version of these materials.

©Copyright Audit Serve, Inc. 2016 – 2018 All Rights Reserved

Post Seminar Handouts
http://www.auditserve.com/ConferencesSeminars/Seminars/Seminar8/tabid/333/Default.aspx

Seminar Design

- Identify all key GDPR Requirements
- Identify Business and IT Impacts
- Provide implementation strategies
- Provide Project Assessments Questions embedded within the discussion of the key regulations
- Discuss GDPR Project Assessment Compliance Levels
- Provide pre-implementation review audit procedures embedded within the discussion of the key regulations
- Does strategy of Post-imp Audit and ongoing recurring compliance audits → Integrated auditing

2

©Copyright Audit Serve, Inc. 2016 - 2017 All Rights Reserved

GDPR

vehicle for putting/ lodging SAR request?

#1 Introduction to GDPR

Q1. Can U process a SAR request?
Q2. How comfortable w/ disclosure process?

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR

- GDPR (Regulation (EU) 2016/679) was adopted on 27 April 2016 in which compliance needs to be achieved by 25 May 2018
- GDPR on 25 May 2018 will replace the 1995 European Data Protection Directive (Directive 95/46/EC).
- Does not require ratification within 28 EU countries
  - Individual countries are changing their data privacy laws to align with GDPR

Directive 95 = 45% of GDPR but no teeth

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Precursor to GDPR

- 1995 Data Protection Directive (95/45/EC) and Directive 2002/58/EC (the ePrivacy Directive)
  - Origin of many of the GDPR requirements
    - GDPR "raises the bar"
    - offers no guidance on penalties
- 28 EU member states and will replace the inconsistent laws the EU member states implemented to comply with the 1995 directive

want for precedences

NY cybersecurity scope:
- Non-public
- encryption
- 2 factor

5

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
What brought about GDPR?

- Monitoring the behavior of EU residents by tracking their digital activities
- The European Union takes a position that privacy is a fundamental right
- No cross-industry privacy laws
  - rules tend to come from industry regulators and state attorney generals
- Need to control that Internet companies that collect and store internally for use in profiling and targeted advertising

6

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR

- What is compelling compliance
  - Financial Penalties
    - financial penalties up to €20m or 4% of annual worldwide turnover for groups of companies
    - Individual data subject lawsuits as per Article 82 - Right to compensation and liability
      - "Any person who has suffered material or **non-material** damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."
      - Class Action lawsuits typical not permitted in EU
        - European Union top courts dismissed Privacy activist class action suit against Facebook
      - Class actions are not permitted in the UK but Group Litigation Order (GLO) allowed
        - GLO allows individuals who have claims which are common can join forces
          - splitting the costs between the group litigants

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

{ controller : Bank, employer
{ processor :
Bidirectional controller - processor
- or -
Recipient of personal data

can sue controller or processor whoever has deeper pocket

Introduction to GDPR

- What is compelling compliance
  - What will be the basis of identifying non-compliance?
    - Internal whistle blower
    - Data Subject Complaints
      - Controllers and Processors not fulfilling Subject Access Rights (SAR) Request
      - All areas where requests can be made not included in Controllers and Processors Subject Access Rights (SAR) Request form
      - Data Subject not provided disclosures by Controller as required by Article 13 & 14
      - Data Subject did not provide Expressed Consent as required by Article 7 & 8
        - Old Expressed Consents inadequate

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Needs expressed consent! whenever there are changes in terms of services

Introduction to GDPR

- Compliance Date: May, 25, 2018
  - Does everything need to be done?
    - Is your company willing to take a risk based approach?
      - Criteria used – What will be seen as non-compliance by Supervisory Authority?
        - Risk of fines
      - Ability to process a SAR Request
      - Processor validation (Article 28)

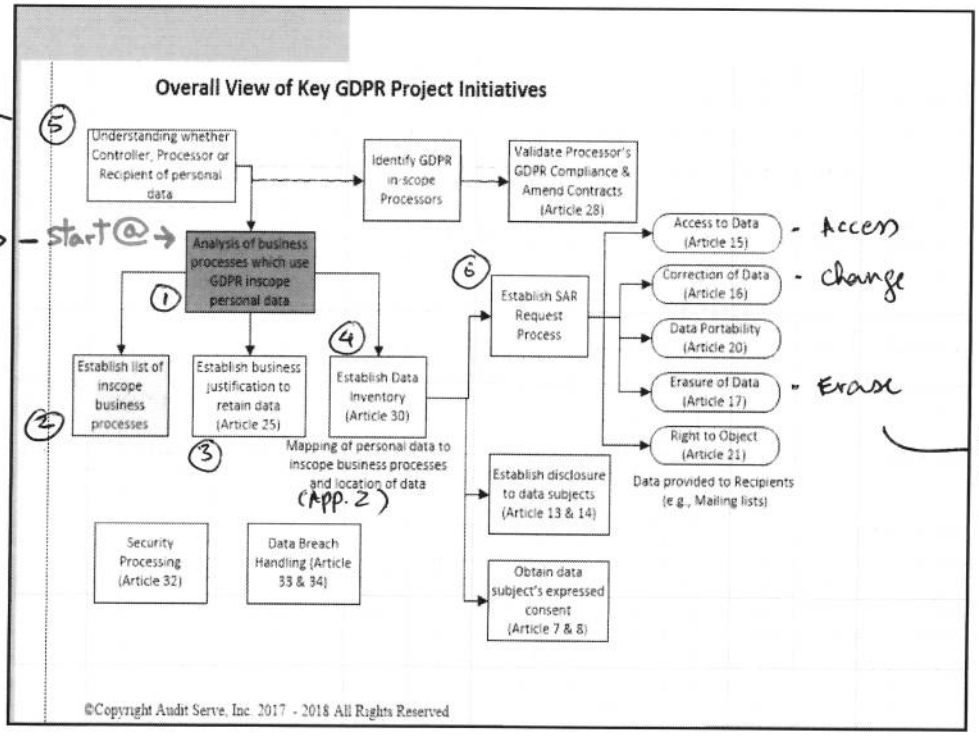
← You cannot use a non GDPR-compliant processor

9

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

c?p?r?

<last, first> – start @ →



©Copyright Audit Serve, Inc. 2017 - 2018 All Rights Reserved

Back Up is not in scope! explicitly in regulations paper not in scope microfiche in scope

Introduction to GDPR

- Who is impacted?

  Article 3 Territorial scope

  "This Regulation applies to the processing of personal data of a controller or a processor regardless of whether processing takes place in the Union or not"

  - Covers all EU organizations which process personal data regardless if they process it in their own facilities located within the EU or using a cloud provider (Amazon Web Services) location outside of the EU

11

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR

- Who is impacted?

  Article 3 Territorial scope

  "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union where processing activities are related to:

  - Offering of goods or services **irrespective of whether payment** of data subject is required

  - Monitoring of their behavior"

  - scope covers all EU citizens' personal data regardless if it is processed by an organization located outside the EU
    - US, Canada or Mexico, etc
  - Covers every imaginable type of business

12

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR

- Who is impacted?

  Article 3 Territorial scope

  "Processing of personal data in the context of activities of an establishment of a controller or processor in the Union regardless of whether processing takes place in the Union or not"

  - Method to tie Hosting providers worldwide

  "Regulation applies to the processing of personal data of data subjects who are in the Union"

  - Interpretation is that EU citizen needs to be domiciled in EU
    - Would lose GDPR rights if they moved outside the EU

subject to debate

13

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR

- Who is impacted?

  Article 3 Territorial scope

  The offering of goods and services irrespective of whether payment of the data subject is required

  "This Regulation applies to the processing of personal data by a controller not established in the Union but in a place where Member State law applies by virtue of public international law"

  - law between sovereign nation-states
    - Method to tie enforcement and compliance worldwide

14

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR

- Who is impacted?
  - companies that do business in Europe
  - Companies that have operations in Europe
  - Companies which store European clients data
  - about 800,000 companies globally.
  - Companies who store or process data of EU residents
  - Company/organization does not need to be registered to perform business in one of the 28 EU countries
  - Organizations who have EU citizen customers regardless if it is a payment of services
  - Any collection on information though a website or social media in which person is a resident of the EU
  - Companies who have employees who are domiciled in the EU

15

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR

- Industries in the US who are impacted?
  - US Colleges
  - Hotels
  - Airlines
  - Casinos
  - Online Merchants (who sell to the EU)
  - Large Retailers
  - Hospitals
  - US companies who have European employers

16

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Key Players

- Data Subject
  - Natural legal person of EU
  - the person legal person whose personal data are collected, held or processed

visitors do not count

17

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Key Players

- Data Controller (referred to in seminar as Controller)
  - Organization or Individual who collect, store or process any data about living people on any type of computer system
  - Control the contents and use of personal data
  - Determines the purposes and means of the processing of personal data
  - Has the most direct relation with Data Subject
  - Required to implement appropriate technical and organizational measures
  - Has obligations on you to ensure contracts with processors comply with the GDPR
  - Data controller remains responsible for the processing although it is carried out by a third party
  - Can also be a "Dual Controller"
    - Distributed model for servicing the data subject

18

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Key Players

- Data Processor (referred to in seminar as Processor)
  - Entity/organization that processes personal data on behalf of the controller
  - Processing by processor governed by contract which requires processor to implement appropriate technical and organizational measures
  - Processors will now have direct obligations and exposure to fines under the new rules
    - Not the case with the current Data Protection Directive
  - Processor could have a direct relationship with the Data Subject

19

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Key Players

- Processor
  - Organization can be both the controller, processor or a 3rd party recipient of data depending on the business process
  - Demonstrate compliance to the controller
    - Right to audit

Example of Processor activities: Process insurance claims

20

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Key Players

- Recipient
  - another body to which the personal data as been disclosed
    - Controller or Processor disclosure of data but not part of the business processing used for services provided to data subject
      - Examples
        - Mailing lists
        - Industry analytics ← insurance analytics although aggregate data still rely on individual data
      - Needs to be disclosed to data subject who has the right to object (Article 21) – *discuss later*
    - Public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients
      - Not included in Controller and Processor Inventory of data
      - But Public Authority must be in compliance with data protection rules

can shutdown this type of business

21

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Key Players

- European Data Protection Supervisor (EDPS)
  - independent supervisory authority at EU level
    - appointed in December 2014 by the European Parliament and the Council of the EU
  - Monitoring the processing of personal data by the EU institutions and bodies
  - Handles complaints and conducts inquiries
  - Advising on policies and legislation that affect privacy
  - Supported by the Office of the EDPS
    - enforcing and reinforcing EU data protection and privacy standards
    - lawyers, IT specialists and administrators

22

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Key Players

- European Data Protection Board (EDPB)
  - Ensure the consistent application and enforcement of the GDPR
    - Suppose to issue guidance for controllers and processors
  - Comprised of EDPS and Article 29 Data Protection Working Party (WP29)
    - an advisory committee comprised of representatives of the EU data protection authorities, EDPS and the European Commission
    - Interpretation and enforcement
    - Provide guidance to processor and controllers to meet GDPR requirements

23

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Key Players

- European Data Protection Board (EDPB)
  - Comprised of EDPS and Article 29 Data Protection Working Party (WP29)
    - Issue Guidance, recommendations and best practices
      - Article 70 - Best Practices

All organizations have the issue that EDPB guidance in future may conflict with project approaches already in place

WP29 Website devoted to providing opinions on achieving GDPR compliance

Limited topics

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

24

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Key Players

- EU Data Protection Authorities (DPAs)
  - enforces data protection law in that Member State
- Supervisory Authority (GDPR Specific)
  - Monitoring the application of GDPR within their member state
  - Each member state provides one or more independent public authority individuals
  - Four year term

25

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Terminology

- Personal Data
  - any information relating to an identified or identifiable data subject
    - an identifiable person
      - identified, directly or indirectly
      - by reference to an identifier
        - Name
        - identification number
        - location data
        - online identifier (cookies)

26

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR Terminology

- Sensitive Personal Data
  - data revealing
    - racial
    - ethnic origin
    - political opinions
    - religious or philosophical beliefs
    - trade-union membership
  - data concerning
    - Health
    - sex life and sexual orientation
    - genetic data
    - biometric data

27

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR Terminology

- Sensitive Personal Data
  - Additional protection measures required
    - Profiling for making automated business decisions
- Anonymous Data
  - Amending data in such a way that no individual can be identified from the data
  - Data is not in-scope for any protection under GDPR

28

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR Terminology

- Pseudonymised Data
  - Linked anonymous data
    - the processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual without the use of additional information
    - anonymous to the people who hold or receive it but contains information or codes that would allow others to identify an individual from it
      - Example: Research team cannot identify individuals but caregivers can identify the individuals they care for
    - identifying fields within a database and replaces them with artificial identifiers/ pseudonyms
    - Mapping table used to link the data
      - Example: a name is replaced with a unique number

29

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

GDPR - Key Regulations

- 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 (Article 8)
- Processing of Special categories (Article 9)
- Right to Erasure (Article 17)
- Processor Requirements(Article 28)
- Right to Object (Article 21)
- Lawfulness of Processing (Article 6)
- Security of Processing (Article 32)
- Data Breach Notification (Articles 33 and 34)
- Data Protection by Design & Default (Article 25)
- Data Protection Impact Assessment (Article 35)
- Automated individual decision making/profiling (Article 22)
- Right to Restriction of Processing (Article 18)
- Recipients of personal data (Article 19)

30

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Understanding the Regulations

- Structure of regulations
  - Definitive requirements which must be adhered to
    - Use the words "shall"
  - Definitive requirements which must be adhered to but provides specific conditions which impacts the degree in which the requirement is to be implemented
    - Use the words "Taking into account"
    - Use the words "risk of varying likelihood and severity for the rights"

Example: Article 32 Security of Processing

Taking into account costs of implementation, purpose of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk

31

©Copyright Audit Serve, Inc. 2016 - 2017 All Rights Reserved

Introduction to GDPR
Understanding the Regulations

- Structure of regulations
  - Definitive requirements but with acceptable approaches provided but accepts alternative solutions

Example: Article 32 Security of processing

Data Controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk

"including inter alia (among other things) as appropriate"

Would deem these measures acceptable but leaves room for other alternatives

"pseudonymisation and encryption of personal data"

32

©Copyright Audit Serve, Inc. 2016 - 2017 All Rights Reserved

Introduction to GDPR
Understanding the Regulations

- Structure of regulations
  - Definitive requirements but "where applicable"
    - Understood that all controllers and processors are not alike and their business process have variations in which regulations would not apply

Example: Article 30 Records of processing activities
Each controller shall maintain a record of processing activities under their responsibilities

Where applicable, transfers of personal data to a third country

Not all controllers transfer personal data

33

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Understanding the Regulations

- Structure of regulations
  - Definitive requirements "where possible"
    - Understood that all controllers and processors are not alike and their business process have variations in which regulations would not apply
    - Understood there are technical limitations to implementing solutions
    - Understood it would not be feasible to change business processes to meet the requirement

Example: Article 30 Records of processing activities
where possible, envisaged (plan/aim) time limits for erasure of the different categories of data

34

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Introduction to GDPR
Understanding the Regulations

- Structure of regulations
  - Regulation allows some latitude for the EU Member States to adopt their own additional rules

Example: Article 8 – Conditions applicable to child's consent in relation to information society services

"the processing of personal data of a child shall be lawful where the child is at least 16 years old. "

"Member States may provide by law for a lower age for the purposes provided that such lower age is not below 13"

35

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

GDPR

#2 Approaches used to perform GDPR Reviews/Audits

36

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Audit Approaches for the GDPR Project

- Typically pre-implementation reviews performed of individual new system deployments
  - GDPR Project involves a pre-implementation review of an entire set of business initiatives to meet the regulations
- Need to make decision if this will be a rated or non-rated audit

37

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Audit Approaches for the GDPR Project

- Alternative Audits that can be performed for the GDPR Project
  - Pre-Implementation Review of the entire lifecycle of the project
    - Auditor involved from project inception through implementation
      - Issue audit reports at various stages of the life cycle of the project
    - Overall Objectives
      - Project Management Review
        - Ensure that the proper project initiatives have been established and are being managed properly to ensure they are completed within the required timeframes to achieve GDPR compliance

38

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Audit Approaches for the GDPR Project

- Alternative Audits that can be performed for the GDPR Project
  - Pre-Implementation Review of the entire lifecycle of the project
    - Overall Objectives
      - Key processes and initiatives are designed properly to meet the GDPR requirement
        - Auditor reviews design and conducts testing/validations to ensure initiatives are properly met

39

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Audit Approaches for the GDPR Project

- Alternative Audits that can be performed for the GDPR Project
  - Post-Implementation Review
    - Combined with the pre-implementation review
    - Overall Objectives
      - Ensure key processes to support GDPR compliance are functioning effectively based on the key processes/controls that were validated during the pre-implementation review

40

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Audit Approaches for the GDPR Project

- Alternative Audits that can be performed for the GDPR Project
  - Standalone Review just prior to required compliance date
    - Point in time review at the later stages of the project
      - Too late to escalate to management that project will not meet GDPR compliance
        - Depends upon if project initiatives are being divided between what is necessary to process a SAR request versus the other requirements of GDPR
      - Key processes and initiatives are designed properly to meet the GDPR requirement
        - Auditor reviews design and conducts testing/validations to ensure initiatives are properly met

41

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Audit Approaches for the GDPR Project

- Alternative Audits that can be performed for the GDPR Project
  - Standalone Post-Implementation Review 1 – 2 months after the compliance date
    - Key processes and initiatives are designed properly to meet the GDPR requirement
      - Auditor reviews design and conducts testing/validations to ensure initiatives are properly met
    - Ensure key processes to support GDPR compliance are functioning effectively
      - Need to establish a list of the key areas
        - Updates to Data Inventory (Article 30)
        - Processing of SAR Requests
        - Processor Validations
        - Data Breach handling

42

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Audit Approaches for the GDPR Project

- Alternative Audits that can be performed for the GDPR Project
  - Ongoing GDPR Compliance Audits
    - Key processes and initiatives are designed properly to meet the GDPR requirement
      - Auditor reviews design and conducts testing/validations to ensure initiatives are properly met
    - Ensure key processes to support GDPR compliance are functioning effectively
      - Need to establish a list of the key areas
        - Updates to Data Inventory (Article 30)
        - Processing of SAR Requests
        - Processor Validations
        - Data Breach handling

43

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

GDPR

#3 Performing a GDPR Project Assessment

44

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

GDPR Project Assessment

- Project Assessment is not intended to be a one-time assessment
- Periodic assessment to measure the progress being made by an organization to reach GDPR compliance
- Define the activities which have been initiated/completed across all areas in-scope for GDPR

45

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

GDPR Project Assessment

- Define remaining project tasks which need to be completed/enhanced within each area which require GDPR initiatives
- Specify the overall state of reaching the goal of complete GDPR compliance
  - Quantitative level assigned to the organization (1 – 7)
  - Each of these compliance levels of achievements map to the most critical aspects of the GDPR project initiatives

46

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

GDPR Project Assessment (Appendix 1)

- Who should conduct the Project Assessment for an organization?
  - Project team
    - Risk & Compliance representation
    - Corporate Legal
    - IT (infrastructure & Development)
    - Business
- Overall basis of validation
  - Project assessments will not approach the level of validation of an audit
  - Will rely on representation of task owners

47

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

GDPR

#4 Understanding the Regulations, Implementation, Assessment and Audit Approaches

48

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Structure of Section

- Go through each of the key GDPR Articles
  - Components specified within each GDPR article
    - Critical components of the Article
      - Exact language used is in quotes
    - Implementation Guidance
    - Key Assessment questions
    - Audit Procedures

49

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

Record of Processing Activities (Article 30)

- "Controller required to maintain a record of processing activities under its responsibilities"
  - Input to achieve requirements within Article 13 & 14 (Data Subject Access to personal data collected by controller)
  - "Purpose of processing"
    - Implementation Guidance: Establish document which describes all business processes across all areas
      - Regardless if it uses personal data
  - "Description of categories of data subjects and of the categories of personal data"
    - Implementation Guidance: Within the document which describes all business processes tied to the data subjects

50

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

Record of Processing Activities (Article 30)

- "Controller and processor required to maintain a record of processing activities under its responsibilities"
  - "Categories of recipients to whom personnel data will or have been disclosed" Specify if third country
    - Disclosure relates to whether data provided to a third party
      - Example: marketing purposes
  - "transfers of data to a third country"
    - Relates to service providers which perform some aspect of processing the data
      - Third party Vendor server/virtualized hosted managed services
      - Third-party Vendor co-location (controllers managed services)
      - Business operation performed by third country

      Will discuss "third country" further in Cross Border Data Transfer

Implementation Guidance: Establish document which ties business processes to systems which are hosted or business processes performed by a third country

51

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

Record of Processing Activities (Article 30)

- "Controller required to maintain a record of processing activities under its responsibilities"
  - Time limits for erasure of different kinds of data
  - Data retention approaches

    Implementation Guidance: Document which defines data retention for all personal data elements as it relates to processing
    - "where possible"
      - But need to substantiate (example of justification: reacquire past customer but for how long?)
        - Further discussed in Article 25

        Cost of implementation "wiggle room"

52

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

Record of Processing Activities (Article 30)

- "Controller required to maintain a record of processing activities under its responsibilities"
  - "general description of the technical and organizational security measures as per Article 32 (security of processing)" – *to be discussed later*
  - Additional Implementation Guidance
    - All the above requirements also pertains to processor performing function on behalf of controller

Project Assessment Questions

Has a project initiative occurred to document all processes performed by the controllers and processors it uses which is tied to the data subjects and whether any of this processing occurs in a third country?

53

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

Record of Processing Activities (Article 30)

- "Controller required to maintain a record of processing activities under its responsibilities"

Project Assessment Questions

Has a project initiative occurred to document all the retention of all personal data as it relates to processing performed of data subjects?

Pre-Implementation Audit Procedures

Review documentation used to support the mapping of processes which collect personal data and trace a sample number of these processes to the documentation established to support personal data used, the data retention and instances in which processes occur at a third country

54

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection by design and by default (Article 25)

Paragraph 1

"the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

- data-protection principles also included as part of Article 32 Security processing – *discussed later*
- Taking is account "cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons"
  - Wiggle room

55

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection by design and by default (Article 25)

Paragraph 2

- "Controller and Processor shall implement appropriate technical and organizational measures to ensure only use personal data which are necessary for each specific purpose of processing are processed"
  - "Amount of personal data collected"
    - Need to have documentation to support each business process which is mapped to the personal data collected
  - " Period of their storage" - Data retention
    - Need to have documentation to support each business process which specifies retention period for personal data collected and provides rational for its retention
  - Data provided to processor and third parties is only what is required
  - How are we interpreting "orphan data" ?
    - data not tied to processing

56

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Not used anymore
project decision delete / not delete

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection by design and by default (Article 25)

"Approved certification mechanisms may be used as an element to demonstrate compliance" - not mandated

- Supervisory Authorities appoint and establish list of independent certified bodies
  - Need to demonstrate compliance (EDPB has not specified criteria)
- Determination needs to be made as whether this certification required before GDPR mandated compliance date
  - Can also utilize other independent mechanisms
    - ISO 27001, SSAE 16, ISAE 3402
      - But the scope of the review may not provide the necessary coverage

SOC 2 has been updated in 2017 to address data privacy

57

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection by design and by default (Article 25)

Ability to "side step" some aspects of the mandate

- "Taking in account the cost of implementation"
  - Can use cost/benefit model
    - Document the costs of implementing the solution in order to "implement appropriate technical and organizational measures"
      - Revisit the costs on an annual basis

New & cheaper technology may become available

58

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

Data Protection by design and by default (Article 25)

Compliance Flexibility

Yes, taking in account the cost of implementation

Project Assessment Questions

Has a project initiative occurred to document all technical and organizational measures to ensure only use personal data which are necessary for each specific purpose of processing which factors data retention requirements and minimum necessary amount of personal data to be used?

Audit Procedures

Perform a review of the documentation created to support Article 25 Data Protection by design and ensure it address all of the requirements.

59

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Information Controllers must provide to Data Subject at time when personal data is obtained (Article 13)
  - "Identity and contact details of the controller, data protection officer"
  - "Purpose of processing related to personal data"
  - "Recipients of personal data"
    - Could be customer of Controller who receives personal data who is not a processor for the Controller
    - Implies also providing list of processors and third-parties who receives personal data

60

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Information Controllers must provide to Data Subject at time when personal data is obtained (Article 13)
  - "Whether personal data it is transferred to a third country"
  - "Retention period of personal data"
  - "Ability to request from controller access to personal data, recertification, erasure and data portability"
  - "The right to withdraw consent"

61

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Information Controllers must provide to Data Subject at time when personal data is obtained (Article 13)

Project Assessment Questions

Has in-person and online methods for acquiring customers been enhanced to provide data subject all the required information mandated by Article 13?

Audit Procedures

1) For a sample number of processes which relate to the data subject acquisition perform observation test of the enhanced online data subject acquisition screens to ensure that data subject is provided all the required information mandated by Article 13.

2) Review documentation provided for in-person acquisition transactions to ensure that the required information mandated by Article 13 are included in the documentation.

62

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Information Controllers must provide to Data Subject where personal data have not been obtained from Data Subject (Article 14)
  - Most scenarios would involve data subject entering in a transaction within controller but personal data obtained from a third party
    - Example: getting a credit report from the credit bureau
  - All information as stated in Article 13 provided to Data Subject
  - Additional information provided to Data Subject
    - Source where personal data originated
    - More details relating to processes using personal data

63

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Information Controllers must provide to Data Subject where personal data have not been obtained from Data Subject (Article 14)

Project Assessment Questions

Have all methods for acquiring customers been enhanced to provide data subject all the required information mandated by Article 14 which includes personal data received from third parties?

Audit Procedures

For a sample number of processes which relate to the data subject acquisition perform observation test (websites, integrated application systems) to ensure that data subject is provided all the required information mandated by Article 14 which includes personal data received from third parties.

64

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Expressed Consent – Article 7
  - "Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing his or her personal data"
  - "The request shall be presented in a manner which clearly distinguishable from the other matters in an intelligible and easily accessible form, using clear and plain language"

65

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Expressed Consent – Article 7
  - What brought about the change?
    - Large agreements not read by consumer
    - Uses ambiguous language that cannot be deciphered
    - Obtaining consumer consent to use their data based on general terms and conditions
    - Data subjects can continuously re-evaluate their consent
  - No Consent by default
  - GDPR does not allow this blanket approach to consent

66

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Expressed Consent – Article 7
  - Consent Practices no longer permitted
    - Opt-Outs by Data Subjects
    - Controller cannot request open-ended consent to cover future processing
    - GDPR does not allow for unambiguous consent
      - GDPR requires consent to be re-obtained each time they have a new use for the customer's data
    - Consumer agreement based on "I Agree" button at the bottom
      - not prefilled radio button

67

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Expressed Consent – Article 7
  - New protections for children by requiring parental authorization prior to collecting and processing the child's data (Article 8)
    - Need business process for collecting parental authorization
  - Organizations may need to get consents again
    - Expressed consents need to re-obtained to cover past consent practices which were not GDPR compliant
      - a project initiative will be required to collect these expressed consents
        - Complication with on-line retail because obtaining re-consent based on customer going to a website
        - In person customers – difficult to track down
      - Will personal data be removed when new expressed consent not obtained?

68

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Expressed Consent – Article 7
  - Data subjects are also given the right to withdraw consent
    - Assume withdrawing consent will not allow business processes to continue and customer will withdraw business from organization
    - Will probably also be combined with having their personal data erased
  - No requirements as a processor to obtain expressed consent from data subject
    - Adds complication to relationship between processor and controller because controller is equally liable as part of Article 82 even if they are not at fault
      - Processors will be demanding contract revisions to ensure that controller has received expressed consents (Article 7,8) and has a lawful basis to process data (Article 6)

69

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Expressed Consent – Article 7

Compliance Flexibility

None, must have data subject expressed consent.

- There is discretion regarding the amount of technical details which need to be provided to the data subject since EDPB has provided no guidance so far.
- Circumstances in which expressed consent needs to be reobtained is not specifically defined in regards to the extent of change in which PI is processed. If sending data to a new third party or processing in different location, that would represent a significant change.
- Whether we need to track PI changes as it relates to the services the data subject uses is questionable versus tracking changes as if data subject uses all services.

70

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Expressed Consent – Article 7

Project Assessment Questions

Has a project initiative occurred to document all consents received and removal of consents?

Assuming original consent does not meet current requirements of Article 7 have project initiatives occurred to obtain the new consent?

Audit Procedures

Perform a review of processes used to track expressed consents which meets the requirements of Article 7

Devise compliance test to ensure that expressed consents obtained

Will require data extracts to perform test

71

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Condition's applicable to Child's consent relation to information society services (Article 8)
  - Information Society Services - any service normally provided for remuneration (money paid) at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, at the individual request of a recipient of the service

"the processing of personal data of a child shall be lawful where the child is at least 16 years old " "Member States may provide by law for a lower age for the purposes provided that such lower age is not below 13"

"controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking in consideration technology"

Will just have a the person certify they are at least the age of 16 within an enrollment process be sufficient?

Any other mechanisms that can used to verify age?

72

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Condition's applicable to Child's consent relation to information society services (Article 8)

  "controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking in consideration technology"

  For validating "holder of parental responsibility" will rely on representation certified as part of the enrollment process?

  How can it be certified they are holder of parental responsibility?

  What happens to historical collections which did not meet standard?

73

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

Lawfulness of Processing (Article 6)

"Processing shall be lawful if following applies (key ones)

- Data subject has given consent
- Processing necessary for the performance of a contract to which the data subject is a party
- Processing is necessary for controller or third party legitimate interest except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data in particular where the subject is a child
  - Who is to refute controller or third party legitimate interest

74

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Condition's applicable to Child's consent relation to information society services (Article 8)

Compliance Flexibility

None

Project Assessment Questions

Has a project initiative occurred to establish system validations to ensure that all data subjects are at least 16 years old?

Has a project initiative occurred to establish an automated and validated collection of parents approval for data subjects which are under the age of 16?

Audit Procedures

Perform an extract of data subjects which are under the age of 16 and ensure that parental approval was obtained.

75

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

Lawfulness of Processing (Article 6)

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent

Additional language to ascertain whether processing for another purpose is compatible with the purpose for which the personal data is initially collected

link between the purposes for which personal data have been collected and the intended future processing

76

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

Lawfulness of Processing (Article 6)

Implementation Guidance

1) Need to identify how all personal data was obtained mapped to the business process to ensure it was for a lawful purpose and purge all other data

- Need to include data provided to processors and third parties

2) If establishing link between past purchase and intended future processing, need to document the basis for the link

Project Assessment Questions

Has the project initiative occurred to review and document all processes which utilize personal data to ensure that all processing was based on the collection of personal based on intended purpose that has not changed?

Audit Procedures

Review documentation used to support the mapping processes which collect personal data and trace a sample number of these processes to the documentation established to support the purpose of processing has not changed

77

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Access by Data Subject – Article 15
  - Data subjects are provided the right of access to their data, and be provided the detailed specifications of how their data is being processed

Implementation Guidance:

- Requires organizations to establish a complete data inventory and data schema
- Documented in a manner which the data subject can understand meaning of all data elements which are stored which represents the data subjects data profile
- Controllers will have to set up a mechanism to respond to these access requests and mechanisms for data subjects to make the requests

78

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Access by Data Subject – Article 15

Project Assessment Questions

Has a project initiative occurred to establish a detailed specification of how a data subject's data was processed.

79

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Access by Data Subject – Article 15

Audit Procedures

1) Review a sample number of business scenarios which relates to the processing of data subject's personal data and determine whether sufficient documentation has been established to meet the requirements of Article 15.

2) For data maintained by processors ensure mechanism established to pull the data to support a right to access request

within 30 days!

80

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Recertification (Article 16)
  - "Data subject will have right to obtain from the controller without undue delay the recertification of inaccurate data concerning him or her"
    - Requirements
      - Provide data subject certification that reports inaccuracies were corrected
      - Undo delay implies within 30 days (not explicit in GDPR)
    - Typical scenarios in which inaccurate data identified which needs to be recertification
      - Cleanup of inaccurate data posted on website
      - Data subject identifying errors of data used for processing based on data subject right to access to obtain data to validate

81

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Recertification (Article 16)

Implementation Guidance:

- Establish process to validate identity of data subject requests
- Establish a detailed procedure based on categories of data inaccuracies of how corrected data will be validated
- Establish proof the data inaccuracies was corrected

Project Assessment Questions

Has a project initiative occurred to establish a process for correct data inaccuracies?

82

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Recertification (Article 16)

Audit Procedures

Perform a review of the formal processes for correcting data subject's data inaccuracies and certification that the corrections were properly made.

83

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Portability – Article 20
  - Provide data subjects the right to request the data controller to provide all of their personal data in structured format that would allow the data subject to transfer their data to another data controller
  - Must at a minimum provide all of the data to the requestor in a machine readable format
  - Request the data controller to directly transfer their data to another controller
    - data controller can reject the request to transfer their data to another controller if it is not feasible

84

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Portability – Article 20
  - Require organizations to establish a complete data profile of the data that they are storing and processing for each type of data subject
    - To what degree is the personal data, data relationships and is it relates to processing documented

85

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Portability – Article 20
  - Require organizations to establish a complete data inventory and data schema
  - Documented in a manner which the data subject can understand meaning of all data elements which are stored which represents the data subjects data profile
  - Difficult for those data controllers which use third-party vendor products in which the software vendor does not publish the data schema they use for the application's database
    - Agreements with third-party vendors/processors will need to be amended to make these data schemas available or these third-party vendors will need to established data repositories derived from the application's databases to allow for the data subject's data to be offloaded upon request

86

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Portability – Article 20

Compliance Flexibility

Yes, controller can reject the request to transfer their data to another controller if it is not feasible

87

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Processing of Special categories (Article 9)

  "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited"

  - Only permitted if (key ones)
    - "Data Subject has given explicit consent"
    - "Processing is necessary for the purposes of carrying out the obligations and exercising rights of the controller"
    - "Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-for-profit "
    - Processing relates to personal data which are manifestly made pubic by the data subject
  - Implementation Guidance: Document all circumstances where this processing of special categories occurs

88

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  under Section 3 Recertification & Erasure
  - "The data subject shall have the right to obtain from the controller the erasure of personal data without undue delay" "data subject withdraws consent on which the processing is based on"
    - Typical scenario - Data subject no longer wishes to do business and they want any trace of their data to removed
    - Request also tied to Article 13 - Information to be provided where personal data are collected from the data subject

89

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  - "the personal data are no longer necessary in relation to the purpose for which they were collected or otherwise processed"
    - Typical scenario – processor no longer doing outsourced activity for controller
    - Implementation Guidance
      - For Controllers and Processors > Track the processes which are no longer used which is tied to a list of data elements which are to be removed
    - Have all traces of the data been erased from a company's records.
    - Need to coordinate with processors
    - Implementation Guidance
      - List of all processors and third parties which also have the data

90

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  - "The personal data have to be erased for compliance with legal obligation in Union or Member state to which the controller is subject"
    - Assumes there are specific laws that limits the length of retention
    - Many laws indicate that data should only retained what is required
    - US NIST cyber security framework is neutral regarding its position on data retention in reverts to established policies

"PR.IP-6: Data is destroyed according to policy" from NIST Cybersecurity Framework

  - US regulations by industry vary which requires retention of customer data even if they are no longer a customer

91

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  - US regulations by industry vary which requires retention of customer data even if they are no longer a customer
    - Employee retention law
      - Occupational Safety and Health Act (OSHA) 5 years
        - Employee health records at place of employment retained 5 years after the period the records relate
        - Log and summary of occupational injuries and illnesses, briefly describing recordable case of injury and illness, extent and outcome of each incident, and summary totals for calendar years
      - Employee Wage and Withholding data (IRS) 4 years
        - Employee ID #, amounts and dates of wages, annuity and pension payment (subset of information) http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Employment-Tax-Recordkeeping

92

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  - "the personal data have been unlawfully processed"
    - Typical scenario – Processor or Controller received private data without legal standing
      - How would data subject know that processor or controller has their data
        - No disclosure as part of acquisition (Article 13)

93

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  - "Where the controller has made the personal data public and is obligated <by data subject request> to erase the personal data"
    - "For exercising the right of freedom of expression and information"

Typical scenario – Google displaying outdated information

This is where right to be forgotten got it origins when Google was displaying inaccurate information regarding a person

2010 Spanish citizen launched complaint against Google Spain that auction notice of his repossessed home displayed on Google search results infringed his privacy rights because proceeding were resolved several years ago and the information displayed was irreverent

based on a search

Court of Justice of the European Union ruled 13 May 2014 that users have the right to ask search engines to remove links when information is inaccurate, inadequate, irreverent or excessive

94

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  - "The controller taking in account of available technology and cost of implementation"
    - Way to get out of complying with data subject request
    - This legal point is the most critical GDPR topic being debated

      If proven that more industries can use waiver will need a document to support that technology not available or excessive cost to implement

95

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  - "Shall take reasonable steps to inform controllers which are processing the personal data that the data subject has requested erasure"
    - Implementation guidance

      Permanent list of controllers and processor in which personal data is shared

96

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  - "The controller taking in account of available technology and cost of implementation"
    - Proof of burden has been shifted to the controller from the 95 Directive
    - Document all technology hurdles
      - Can't delete data from backup tapes
      - Need to change data structure and business processing
        - Business requires name of loan guarantor for processing a loan request

        If guarantor "right to be forgotten" business process fails
      - Document excessive implementation costs

97

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  - What proof is required to the data subject?
    - Minimum level
      - Overall certification that all data has been removed from controller/processors systems and all third-parties in which data was shared

98

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)
  - What proof is required to the data subject?
    - Additional level
      - Specifications of where data was deleted from

        Databases, unstructured data, third party providers

        Implementation Guidance: Restructure contracts with third parties in which data is shared to require them to provide certificate upon request to delete data subject's data

99

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)

Compliance Flexibility

The controller taking in account of available technology and cost of implementation

Project Assessment Questions

1) If controller is waiving compliance based on unavailable technology or cost of implementation, has a document been established to support these contentions.

2) Has a business process review been conducted to identify instances where business processes will no longer operate if right to erasure was permitted

100

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Erasure/Right to be forgotten (Article 17)

Audit Procedures

Assess the adequacy of documentation to support the controller contention of unavailable technology or cost of implementation.

101

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Automated individual decision making/profiling (Article 22)
  - Data subject shall have the right not to be subject to a decision based solely on automated processing including profiling
    - Typical scenarios: rejecting loan application based on economic level of the neighborhood
    - Does not apply if data subject provides explicit consent
    - This starts 25 May 2018 and does not impact processing but impacts legacy processing once after 25 May 2018
  - Implementation Guidance: Document all automated processes driving business decisions which includes instances of profiling

102

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Automated individual decision making/profiling (Article 22)
  - "Shall not apply if necessary for entering into, or performance of a contract between the data subject and the data controller"
    - Controller could not chose to do business with data subject unless they agree to provide consent "wiggle room"
  - "Is based on data subject's explicit consent"
    - Controller could not chose to do business with data subject unless they agree to provide consent

103

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Automated individual decision making/profiling (Article 22)

Project Assessment Questions

1) Has a project initiative occurred to document all automated processes driving business decisions which includes instances of profiling.

2) Determine legal basis for automated processes driving business decisions which includes instances of profiling and if not, obtain consent from data subjects or determine legal path for updating existing contract

Audit Procedures

Perform a review of documentation to support the use automated processes driving business decisions which includes instances of profiling.

104

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Restrict Processing (Article 18)
  - Data Subject right to restrict processing by the controller based on specific situation
    - Contesting the accuracy of personal data
    - Processing is unlawful
  - When processing restricted, Controller can only process with data subject consent
    - "with the Exception of storage
      - Interpretation: Can still perform data backups

105

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Restrict Processing (Article 18)
  - Data Subject right to restrict processing by the controller if unlawful or inaccurate

Compliance Flexibility

Yes, prove lawful processing

106

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Object to Processing (Article 21)
  - Data subject right of object to processing of personal data on the grounds of "relating to his or her particular situation"
    - Processing for direct marketing purposes
  - If processed for scientific, historical or research purposes
    - Exclusion over data subjects objections if processing is for a task for reasons of public interest

107

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Object to Processing (Article 21)
  - Basis of discovery by data subjects
    - Right to Access – Article 15
      - Information to be provided where personal data are collected from the data subject
    - **Article 13 -** Information Controllers must provided to Data Subject at time when personal data is obtained

108

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Right to Object to Processing (Article 21)

Compliance Flexibility

- Partially, exclusion over data subjects objections if processing is for a task for reasons of public interest.
- Controller can choose not to comply if it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject
- Data subject in all cases can restrict processing where personal data is processed for direct marketing purposes

109

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Establishing a Subject Access Rights (SAR) Request Process
  - Which articles the SAR Request Process Cover?
  - What will be the method for authenticating the requestor?
    - Establish a process/system to validate the identity of a data subject prior to processing their request
    - Ensure that the identity management system address all categories of data subjects
    - Timeline to process a request does not start till identity validated
  - May want to authenticate the requestor first and them provide a list of areas they can make their request based on the services they used
    - May not be wise to publish the list of all areas that SAR requests can be made that is accessible to the general public

110

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

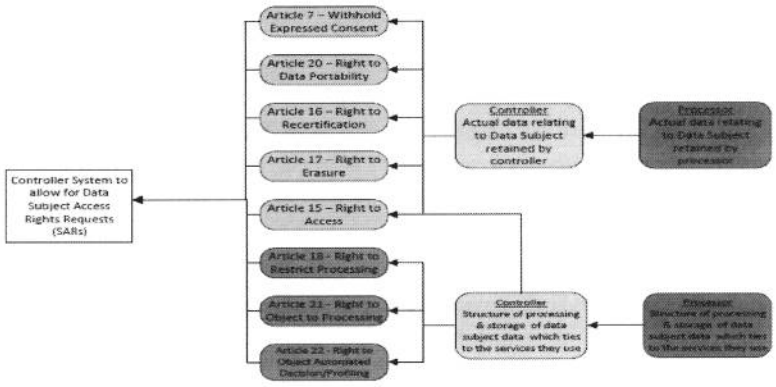
- Establishing a Subject Access Rights (SAR) Request Process
  - Mechanism used to make the request
    - Website
    - Email mailbox
    - Phone
    - Mail
  - Use of third party service providers
  - Complications when dual controller
  - Processors also need to be prepared to receive SAR requests

111

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

GDPR Required Data Subject Rights (SAR) Request Systems



©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Recipients of personal data (Article 19)
  - Processor and Controller will need to track recipients that were provided personal data
  - Controller needs to notify recipients of personal data in which data subject requests occurred for
    - Right to Recertification (Article 16)
    - Restriction of processing (Article 18)
    - Right to Object Processing (Article 21)
    - Right to Erasure (Article 17)
  - "unless this proves impossible or involves disproportionate effort"
    - Will need to document this justification
  - Data subject can request controller to provide disclosure of recipients that were provided personal data

113

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Recipients of personal data (Article 19)

Project Assessment Questions

Has a system been deployed which systematically alerts all recipients of personal data when the data subject requests Right to Recertification (Article 16), Restriction of processing (Article 18) and Right to Erasure (Article 17) to ensure they take the required measures

Audit Procedures

Perform a review of the system deployed which provides notification to recipients of personal data to ensure and effective set of controls and procedures are established to ensure that requirements of Article 19 are enforced.

114

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification – Article 33, 34
  - "a breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or processed" GDPR
    - any information relating to an identified data subject which will increase the number of conditions in which breach notification will be required
    - What is the definition of a data breach?
      - Opportunity or taking advantage of an opportunity

      Most organizations define a breach as having opportunity which does need to be confirmed that it actually occurred

      If inadequate audit trails will never know if took advantage of opportunity

115

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification – Article 33, 34
  - This scope of the GDPR personal data breach goes beyond the breach definition of GLBA, HIPAA and State privacy/breach notification laws.
    - US-based laws/directives focus strictly on breach notification for accidental & unauthorized disclosure but not for destruction or alteration of personal data
    - Accidental deletion or change of an attribute of individual's personal information would now require escalation within an organization to allow the data controller to notify the supervisory authority and the impacted individual (i.e., data subject)

116

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification – Article 33,34
  - Notification is required no more than 72 hours after having "**become aware**"
    - If organization does not have effective audit trails and review processes they may never "become aware"
    - Require organizations to establish an organizational structure which extends to the lowest levels of an organization to ensure that all inappropriate disclosure, alteration or deletion of personal data are identified and escalated to the data controller
      - Mechanisms also need to be extended to all third-parties used by the data controller in which personal data is shared
        - Requires contract provisions in place to ensure the third-parties are required to notify the data controller of each individual incident of a data breach
        - Data controller should also perform independent reviews to ensure the third-parties have these control measures in place

117

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification
  - GDPR uses the words "access to" which implies that if a person had inappropriate access to the data
    - Examples of situations which may be considered a breach
      - Inappropriate access identified during an access recertification review
        - if there were no audit trails to support that the person did not use this access, then it could be interpreted that this type of situation would need to be reported as a security breach
      - use of an emergency ID by a support person (e.g., to make a direct change to data) which has global privileges to view or alter data.
        - Since in most organizations, audit trails have not been established at the database table/record level to identify the data that was accessed or altered, there would be no ability to determine whether an unauthorized disclosure, alteration or deletion of personal data occurred.

118

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification
  - Standards to be established to determine the type of situation in which accidental/unauthorized disclosure or alteration of data is considered an "actionable" case which needs to be reported as a security breach
    - Limited guidance provided at this point by EDPB/Working Party 29

119

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification
  - Define what constitutes unauthorized disclosure

Most common instances in which unauthorized disclosure would occur:

- An individual having access rights to personal data which is not required for their job function which would be disclosed by the periodic access recertification reviews which are performed
- unauthorized takeover of a human or service account which has access rights
- Accidental release of personal data in an email sent by personnel
- Lost laptop or flash drive that is not encrypted
- Movement of personal data from secured locations to unsecured locations by those individuals authorized to have the access (would be controlled by future DLP controls)

120

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification
  - GDPR uses the words "access to" which implies that if a person had inappropriate access to the data
    - Examples of situations which may be considered a breach
      - Inappropriate access identified during an access recertification review
        - if there were no audit trails to support that the person did not use this access, then it could be interpreted that this type of situation would need to be reported as a security breach
      - use of an emergency ID by a support person (e.g., to make a direct change to data) which has global privileges to view or alter data.
        - Since in most organizations, audit trails have not been established at the database table/record level to identify the data that was accessed or altered, there would be no ability to determine whether an unauthorized disclosure, alteration or deletion of personal data occurred.

121

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification – Article 33, 34
  - GDPR provides a key exception to the breach notification reported to the supervisory authority in a situation where the personal data breach is unlikely to result in "a risk for the rights and freedoms of natural persons"
    - organization needs to establish their own risk assessment process to drive the decision as to risk level of each incident
      - Audit Serve Recommended Factors
        - Type of data
        - How many?
        - To whom (insider, outsider, third-party)

122

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification – Article 33, 34
  - GDPR Data Breach Requirements also requires coordination with our Processors which handle personal data
    - Contract updates to ensure the processors report the breach within 48 hours (assume this number based on controller requiring to report breach to Supervisory Authority within 72 hours)
    - A decision needs to be made as to whether processors will be required to accept to accept Controller's definition of a breach
    - Who will be performing Risk Assessment of personal data breaches to determine whether it needs to be reported?

123

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification – Article 33, 34

Project Assessment Questions

1) Has an organizational structure been established to allow for 72 hour escalation of security breaches

Has GDPR Breach notification process been integrated with the existing Incident management process?

2) Has a project initiative occurred to document all types of situations which would warrant the escalation a security breach

3) Has a project initiative occurred to ensure that processors will escalate to the controller within the required timeframes

4) Has a Risk Assessment framework been established to determine whether breach needs to be reported?

5) Is there a process to document all potential breaches?

124

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Breach Notification – Article 33, 34

Pre-Implementation Audit Procedures

1) Conduct a review of the types of situations which would warrant the escalation a security breach and conduct sample testing to determine whether these incidents would be escalated.

2) Conduct a review of the escalation process to ensure that is designed to ensure that all security breaches would be escalated.

3) Conduct a review of the risk assessment process established to determine whether a breach needs to be reported and determine whether it covers all factors?

125

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Security of Processing (Article 32)
  - GDPR Mandates
    - "Data Controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk"
      - Taking into account cost of implementation
      - Some Risk Acceptance allowed
      - Use of Risk Assessments to determine the level of controls which need be established
        - ISO 27005 Risk Assessment would meet all the requirements of Article 32
        - Alternative is a combination of Enterprise, Application and component level Risk Assessments

126

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Security of Processing (Article 32)
  - GDPR Mandates
    - "including inter alia (among other things) as appropriate"

    Would deem these measures acceptable but leaves room for other alternatives
    - "pseudonymisation and encryption of personal data"
      - Reduces risk or appropriate level of security?
    - "The ability to ensure ongoing confidential, integrity, availability and resilience of processing systems and services"
      - Impact types within a risk assessment
      - Organizations will still need document controls established at network, OS, DB and Application layers

127

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Security of Processing (Article 32)
  - GDPR Mandates
    - "The ability to restore the availability of access to personal data in a timely manner"
      - Organizations will need to document their RTO and RPO as it relates to all processes which contain personal data
    - "A process for regularly testing" – to ensure the accuracy of data
      - Organizations will need to document their test methodologies

128

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Security of Processing (Article 32)
  - "accessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing"
    - Implies Risk Assessments
      - What will the areas be in scope for the risk assessment
        - IT Domains: Network, OS, DB, Application, Unstructured Data
        - Business Domains: Business processing (covered in Integrated Audits)

129

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Security of Processing (Article 32)

  Compliance Flexibility
  - No guidance provided by EDPB
    - With no guidance, organizations have discretion on how far they will take technical and organizational measures
  - Core requirement for both Controllers and Processors.
    - As part of Controller's Article 28 oversight of Processor should request details of how compliance is achieved

130

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Security of Processing (Article 32)

Project Assessment Questions and Audit Procedures

Has a project initiative (Risk Assessments) occurred to document all technical and organizational measures that have been implemented to ensure a level of security appropriate to the risk

131

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection Impact Assessment (Article 35)
  - "The controller shall prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protections of personal data"
  - "Where a type of processing in particular using new technologies"
    - Interpretation – new underlining technology used or new application which involves personal data
      - Is it considered new if introduced after GDPR implementation date?
  - "In particular"
    - Interpretation – makes all new technology is scope but also draws in legacy applications/technology

132

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection Impact Assessment (Article 35)
  - "Taking in account the nature, scope, context and purpose of processing, is likely to result in a high risk to the rights and freedoms of natural persons"
    - Interpretation – If risk assessment framework used in which risk of application/technology is not high then Data Protection Impact Assessment not required to be performed

133

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection Impact Assessment (Article 35)
  - GDPR does not mention use of frameworks to create Data Protection Impact Assessment
    - UK PIA code of practices issued by ICO is a good starting point

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

134

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection Impact Assessment (Article 35)
  - "The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68."
    Waiting for the supervisory authority to establish
  - Implementation Guidance for identifying potential in-scope areas
    - Establish inventory of all business processes which involve personal data
    - Map the business processes to the applications & databases they use

135

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection Impact Assessment (Article 35)
  - GDPR Guidance for assessment
    - A systematic description of the envisioned processing operation
    - An assessment of the necessity of the processing operation in relation to its purpose
    - An assessment of the risks and freedoms to the data subjects
    - Measures to address the risks – mechanisms to ensure the protection of personal data

136

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection Impact Assessment (Article 35)
  - Implementation Guidance for performing Data Protection Impact Assessment
    - Based on the handling of data subject data establish risks related to identifying all paths to access the data of the data subject
      - Data Input functions which involve data of consequence
      - Any direct database access to database tables which store the data consequence
      - Identify program and system process ability to access data of consequence which are not controlled through system processes
      - Specify any third-party ability to access the data
      - Establish an assessment of the risks and freedoms to the data subjects
    - Document the adequacy of security to these paths of access and identify areas where additional containment measures need to be established

137

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Data Protection Impact Assessment (Article 35)

Project Assessment Questions

Has a project initiative occurred to conduct a data protection Impact Assessment new high risk operation processes?

Audit Procedures

Select a sample number of a data protection impact assessments that were performed in determine whether a framework was to produce the results.

138

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Processor (Article 28) under Chapter IV Controller and processor
  - "Controller shall only use processors providing sufficient guarantees to implement appropriate technical and organizational measures that requirements will meet the requirements of this Regulation and ensure protection of the rights of the data subjects"
    - Due diligence review of processor before entering into a contract
      - Part of Vendor Management

139

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Processor (Article 28) under Chapter IV Controller and processor
  - "Processor shall not engage another processor without prior written authorization of the controller"
    - Assumes a processor who performs a unit of work on some integrated application hosted at the Controller
      - Will not include using staffing agency to augment resources that perform work at the processor
    - Which subcontracted/outsourced services used by Processor comes under this?
      - Technology services used by processor?
        - Example: Processor use of Azure, AWS to host application processor manages in behalf of Controller

140

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Processor (Article 28) under Chapter IV Controller and processor
  - "Processor shall not engage another processor without prior written authorization of the controller"
    - Implementation guidance
      - Document definition and criteria used to identify processors
      - Track Processors used by processor and disposition of controller approval

141

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Processor (Article 28) under Chapter IV Controller and processor
  - "Processing by a processor shall be governed by a contract"
    - Implementation guidance
      - Verify that contracts are in place

142

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Processor (Article 28) under Chapter IV Controller and processor
  - Does controller have requirement "delete or return all personal data to the controller after the end of the provision of services unless member state requires storage of personal data"
    - Determine whether processor that the processor uses stored personal data
    - Implementation guidance
      - Maintain Inventory of processes mapped to data inventory/personal data, performed by Processor and processor that processor uses
      - Assess mechanisms which ensures that personal data is deleted
        - Automated process which deletes data
        - Certification that data was deleted at the end of services

143

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Processor (Article 28)
  - Validation of processor's GDPR Compliance
    - Need to establish scope of Due Diligence review to evaluate vendor based on type of vendor
      - Ability to process SAR requests
      - Compliance with data removal requirements of Article 25
      - Assess processor interpretation of the design and implementation requirements for Article 32
      - Assess Breach notification process
        - Determine mechanisms Processor established to define a breach
        - identify a breach
        - escalate a breach
        - conduct risk assessment to determine whether breach needs to be reported

144

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Processor (Article 28)
  - Validation of processor's GDPR Compliance
    - Need to establish mechanism to conduct the due diligence reviews
      - GDPR compliance Questionnaire that Processor completes
        - May be interpretation of questions
        - No ability to validate whether responses are accurate
      - Onsite meetings with processor
      - Request vendor to present specific deliverables
      - Independent 3rd party audit

145

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Cross Border Data Transfer
  - Prevents EU Data subject from being transferred from with EU countries to third countries that do not have equivalently strong data protection standards

146

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Cross Border Data Transfer
  - Alternatives
    - Article 45 – Transfers on the basis of EU adequacy decision - Country level agreement
      - Transfer of personal data to third country when the third country satisfies adequate level of protection
        - Allows for controllers and processors within the third country to operate under this mechanism with additional certifications

147

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Cross Border Data Transfer
  - Status of other Countries http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
  - For Directive 94/46/EC flow of EU data from 28 EU countries and three EEA member countries (Norway, Liechtenstein and Iceland) which provide an adequate level of protection (as of 24 NOV 16)
    - Andorra, Argentina, Canada (commercial organizations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay

148

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Cross Border Data Transfer
  - Alternatives
    - Article 46 – Transfers subject to appropriate safeguards – Model Clauses
      - Transfers allowed based on standard protection clauses which have been approved since Directive 95
        - Could be amended by GDPR – not yet
        - Same binding corporate rules in accordance with Article 47
      - Does not require approval from Data Protection Authority

149

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Cross Border Data Transfer
  - Alternatives
    - Article 47 – Cross Broder data transfer within a corporate group (group of enterprises engaged in a joint economic activity) - Binding Corporate Rule
      - Need to specify
        - general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default
        - the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question
        - the rights of data subjects in regard to processing and the means to exercise those rights
      - Requires approval Data Protection Authority

150

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Cross Border Data Transfer
  - EU-US Privacy Shield
    - agreed to on 2 February 2016
    - reflects the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbor framework invalid
    - 12 July 2016 approval of the EU-U.S. Privacy Shield Framework
      - Commerce Department started accepting certifications on 1 August 2016
    - Does not meet all GDPR requirements
      - Was written to meet 1995 Data Protection Directive (95/45/EC)
      - Will there be pressure in future to upgrade Privacy Shield?

151

©Copyright Audit Serve, Inc. 2016 - 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Cross Border Data Transfer
  - EU-US Privacy Shield
    - Requirements of the Organizations
      - Organization must fall under the enforcement authority of a U.S. agency to ensure compliance
      - It must publicize its commitment to adhere to the Privacy Shield Principles
      - Publicly disclose its privacy policy
      - Implement the Principles

152

©Copyright Audit Serve, Inc. 2016 - 2017 All Rights Reserved

Understanding the Regulations, Implementation, Assessment and Audit Approaches

- Overall Summary of Cross Border Data Transfer as it relates to US
  - Privacy Shield used by companies that need to transfer data from EU to US
    - Example:
      - Global company that needs to pass data relating to their EU employees to US where HR processing takes place
      - Global company that needs to pass data relating to their EU customers to US where processing takes place
    - Differences between GDPR as compared to 1995 Data Protection Directive
      - EU employees who work in EU and customers in-scope for GDPR will need to be made aware that their personal data is being sent from EU to US
    - Privacy Shield does not provide data subjects all GDPR rights

153

©Copyright Audit Serve, Inc. 2016 – 2018 All Rights Reserved

GDPR

#5 Data Protection Officer

154

©Copyright Audit Serve, Inc. 2016 – 2018 All Rights Reserved

Understanding the role of the Data Protection Officer

- Who requires a Data Protection Officer?
  - Article 37 requires controllers and processors of personal information to designate a data protection officer when the processing is carried out by a public authority or when "core activities" require "regular and systematic monitoring of data subjects on a large scale" or consist of "processing on a large scale of special categories of data"
  - "Estimated 28,000 data protection officers (DPOs) will need to be hired in the next two years in Europe and the US" Internal Association of Privacy Professionals

155

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the role of the Data Protection Officer

- Data Protection Officer Responsibilities
  - to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to the GDPR
  - to monitor compliance with the GDPR, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits
  - Ensure that the data protection impact assessment is completed and monitor its performance
    - Ensure remediation issues are tracked and resolved

156

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the role of the Data Protection Officer

- Data Protection Officer Responsibilities
  - to act as the contact point for the supervisory authority on issues related to the processing of personal data
  - Contact of data subjects
    - Required to provide Data Subjects name of DPO
    - Organizational decision on whether DPO will have role in any aspect of Data Subjects requests as part of their Access Rights

157

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Understanding the role of the Data Protection Officer

- Where its sits within your organization
- Determine data protection authority you come under
  - International organization

158

©Copyright Audit Serve, Inc. 2016 – 2017 All Rights Reserved

Conclusion

- Questions?
- Feel free to pick my brain in the future Levinemh@auditserve.com
- Subscribe to our free monthly newsletter Audit Vision @ www.auditserve.com which has been published since 1991 and join 3,500 other subscribers -*We do not sell or distribute our subscriber list*

159

©Copyright Audit Serve, Inc. 2016 - 2018 All Rights Reserved

Appendix 1

Audit Serve's GDPR Project Assessment
Compliance Level Scorecard for Controllers

Level	Task	Target Date
0	No formal GDPR activities (No Project Sponsor, No GDPR Project Manager appointed)	
1	* Project Sponsor appointed * GDPR Project Manager appointed Data Protection Officer appointed Project Impact Analysis initiated Permanent Project Binder to support GDPR compliance	March, 2017
2	* Project Impact Analysis completed * Initial Project Plan established for identifying GDPR project initiatives * All in-scope GDPR business processes identified All processors of inscope GDPR processes are identified All third party vendors who support in-scope GDPR processes are identified All third party recipients of in-scope GDPR data are identified Legal interpretation completed of all Articles to validate GDPR in-scope activities *Organizations role as a processor, controller, third-party or recipient of data subjects' personal data are identified	May, 2017
3	* Project plan updated to capture all tasks required to complete the GDPR project Identify vendor contracts which need to be changed to achieve GDPR compliance	June, 2017
4	Alternative methods required to capture Data Subject requests are defined Recipients of all personal data identified *Location of all personal data within business processing identified *Location of personal data within structured data environment identified as it relates to business processes Location of personal data within unstructured data environment identified as it relates to business processes Requests made to processors to obtain their mapping of personal data to business processes *Mapping of processes to Data Subject's personnel data completed (Article 30)	October, 2017
5	*Inventories established and decisions made as to data which will be made accessible to data subject for Data Access Rights (Article 15) and Recertification (Article 16) , Data which can be requested for removal based on exceeding required retentions (Article 25), data which will be available for data portability (Article 20), and data subject Right to Erasure (Article 17) *Inventories established and decisions made as to rights to data subject to object to (Article 21) business processes, sharing of data with third party recipients and data subject communications. Documentation established to provide reason for not providing data subject rights as part of Article 15, 16, 17, 20 and 21) Documentation established to support instances where purging of data cannot occur for data retained beyond business requirements Article 25) Systems and processes have been deployed which provide the ability for data subjects to make requests under Article 15, 16, 17, 18, 20, 21,22	January, 2018
6	*Systems and processes have been deployed which allow for compliance with Article 7 & 8 * Validation systems have been deployed to authenticate the identity of data subjects making requests *Personal data is removed and processes shutdown that prevents GDPR compliance from being achieved *Systems and processes have been deployed which provide required disclosures at the time of first data subject contact (Article 13,14) *Data Extracts or data subject self-service model established to allow for access to data (15), recertification (16) and Data Portability (20) *Processor GDPR compliance validated * Data Breach notification procedures updated and personnel trained * All business changes have been implemented to support GDPR compliance * All IT changes have been implemented to support GDPR compliance GDPR compliance monitoring implemented Data Protection Impact Assessment performed for new high risk processes Data Breach escalation process tested	April, 2018
7	* Dress Rehearsal completed which validates that all business processes and IT processing which allow for GDPR compliance to be achieved have been validated * Project sponsor signs-off on GDPR compliance	25 May 2018

Legend * show stopper, drop one level if not completed

Target Date – The target date is the recommended date for completion of the level based upon completing all GDPR project initiatives by 25 May 2018

©Copyright Audit Serve, Inc. 2017 All Rights Reserved

p30 Key GDPR Regulations

Appendix 2a

GDPR Personal Data Inventory

Business Process	SubProcess	Source of Personal Data Provided by Data Subject	Personal Data Provided by Data Subject (Article 13)	Optional/Required Entry	Database	Table Name	Column Name	Personal Data not provided by Data Subject (Article 14)
Membership Management (enrollment and modifications)	Enrollment	Organization Website			XXXX DB			
			First Name	Required		Person	FirstName	
			Middle Name	Optional		Person	MiddleName	
			Last Name	Required		Person	LastName	
			Birth Date	Required		Person	Birthday	
			Gender	Required		Person	Gender	
			email address	Required		Person	Email1	
								Join Date
			Occupation	Optional		FunctionRole	Name	
			Address	Required		Address	Address1	
			City	Required		Address	City	
			State	Required		Address	StateProvince	
			Postal Code	Required		Address	Postal Code	
			Work Phone	Optional		PhoneNumber	Phone	
	Modification	Data provided Member via email correspondence, phone call	All fields within "Add Member"	See above	XXXX DB	See above	See above	None

These seminar materials are to be used for your personal use only as a registered attendee of the ISACA GDPR Seminar and cannot be redistributed to anyone else or posted on any website or in the cloud. No software is to be used create a non-password protected version of these materials

©Copyright Audit Serve, Inc. 2016 – 2018 All Rights Reserved

* structured + Unstructured Data
scope – tied to business process?
Is it personal or part of / context of business?

Appendix 2 b

Database	Table Name	Column Name	Retention Justification (Article 25)	Recipients of the personal data	Other locations where unstructured personal data stored
			All data is required while data subject is an active member. When data subject is no longer a member then the member is defined as inactive and all data subject data will be removed within 90 days.	No One	Extract of active members stored on Member Services departmental share monthly
XXXX DB	Member	Join Date			
	N/A	N/A	All data is required while data subject is an active member. When data subject is no longer a member then the member is defined as inactive and all data subject data will be removed within 90 days.	No One	email from members regarding changes to their account information are stored on common email folder restricted to Member Services

Appendix 3 - Disclosure

Personal Data Disclosure to Data Subject - Article 13, 14, (Disclosures to Data Subject at time when personal data obtained) and 7 (Expressed Consent)
Also to be provided based on SAR from Data Subject - Article 15 (Right to Access)

Business Process	Personal data Collected from Data Subject (Article 13 which is tied to the Article 7 Expressed Consent)	Personal data created by organization (Article 14 which is tied to the Article 7 Expressed Consent)	The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Article 25)
Membership Management (enrollment and modification and drop)	New membership requires the Organization to collect personal data which is stored on the organization's database system comprised of Name, Birth Date, Gender, address information and Join date.	When an individual becomes a member the system generates the Join Date.	All data is required while data subject is an active member. When data subject is no longer a member then the member is defined as inactive and all data subject data will be removed within 90 days.

Additional Article 13 requirements to be included in the overall disclosure

1) Identity and the contact details of the controller and, where applicable, of the controller's representative;
2) The contact details of the data protection officer
3) Statement that the controller does not intend to transfer personal data to a third country or international organisation
4) Statement that there is an a existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

These seminar materials are to be used for your personal use only as a registered attendee of the ISACA GDPR Seminar and cannot be redistributed to anyone else or posted on any website or in the cloud. No software is to be used create a non-password protected version of these materials

©Copyright Audit Serve, Inc. 2016 – 2018 All Rights Reserved

ISACA®

Trust in, and value from, information systems

Greater Hartford Chapter

CERTIFICATE OF ATTENDANCE

CPE Credits: Up to 8

Event: "GDPR"

Date: Wednesday, April 11, 2018
Time: 8:30 AM - 5:00 PM
Attendee: **Hoang Vinh Nguyen**
Authorized by:

Penette Van Menxel

Penette Van Menxel
Secretary, Greater Hartford Chapter – ISACA