Navigating Privacy Shield and the EU GDPR

Data Security and Privacy Challenges US and Transatlantic entities need to know

Goal

- To convey in 1 hour an overview of the essence of what I have learned about GDPR and Privacy Shield

- However, if you like this topic and want to participate in a workshop, let Greg Streder know, and we can likely make that happen.

Introduction

- Harvey Nusz, CISSP, CIPM, CISA, CRISC, CGEIT
- PrivacyShieldGDPR@gmail.com
- 832-858-9205
- Background:
  - Privacy, Privacy Shield / GDPR, IT Risk Management, IT and Cyber Security, Disaster Recovery / Business Continuity, Governance, Compliance, Identity Access Management, IT Audit, Program Management, Security Architecture
  - ISACA, Greater Houston Chapter, President
  - IAPP, Houston, KnowledgeNet Chair
  - ISSA, South Texas Chapter, Past President

Today

- Very happy to be here, a place I have visited before as a guest, plus I know your wonderful Board Members, or most of them. ☺
- Privacy is Serious Business in Europe because many lives were lost due to being able to find and kill / purge… people. This is quite different from our U.S. perspective; we need to keep this in mind.
- Servant Leadership… being other directed….

How I Got Into Privacy and GDPR

- Finished a consulting assignment on IAM in Keller, Tx, in late July, 2015
- Planned to stay in IAM, but a Privacy position was made available, prepping for GDPR…
- That was in August of 2015
- In October, 2015, Safe Harbor was declared invalid… a sea change….
- And I started signing up for GDPR courses….
- And applied to speak at ISC2's 2016 Security Congress

Who Must Comply with GDPR?

- If you are sending EU Citizens' privacy data to the US, or storing their privacy data from their visits to your website, you will be subject to the EU General Data Protection Regulation (GDPR) by May 25, 2018.
  - IP Address – will be privacy related in GDPR
- This is a culture change, requiring a program, not just a project, to implement.
  - Drucker – Culture eats strategy for breakfast
  - A Leadership Conference in Lisbon I attended in 2016
- Fines can range up to 4% of Worldwide Gross Sales, based upon last years financials.

The Human Rights Commission

- Circa 1950
- Right after WWII
- My own experience
- This is a culture change, requiring a program, not just a project, to implement.
  - Drucker – Culture eats strategy for breakfast
- Fines can range up to 4% of Worldwide Gross Sales, based upon last years financials.

High Level Timeline

- EU Directive, 1995
- Safe Harbor, 2001
- Cookie rules, 2009
- Snowden…
- Safe Harbor is Invalidated, 10/2015
  - Max Schrems, Austria, Privacy Activist and Attorney
- Privacy Shield is Announced, 02/2016, then goes dark due to disagreement with it
- GDPR is Passed, 4/14/2016
- Privacy Shield is Suddenly Announced in early July, 2016 – The advantage of applying before sept 30 2016

Privacy Shield, MCCs, or BCRs?

- If you transferred EU Citizen's Privacy Data from the EU to the US, and are storing that data here, and are doing an Onward Transfer to business partners, you need a method to do this.
  - Privacy Shield
    - A detailed Privacy Policy – actually a notice – with the Privacy Principles, and contracts with your vendors.
    - It starts you down the road toward GDPR
    - Lawsuit – plus the one year review is coming up
  - Model Contract Clauses
    - Lawsuit
  - BCRs
    - In the GDPR.

Privacy Shield Principles

- Notice
- Choice
- Accountability for Onward Transfer
- Security
- Data Integrity and Purpose Limitation
- Access
- Recourse, Enforcement, and Liability

Privacy Shield Supplemental Principles

- Sensitive Data
- Journalistic Exceptions
- Secondary Liability
- Performing Due Diligence and Conducting Audits
- The Role of the Data Protection Authorities
- Self-Certification
- Verification

Privacy Shield Supplemental Principles

- Human Resources Data
- Obligatory Contracts for Onward Transfers
- Dispute Resolution and Enforcement
- Choice -- Timing of Opt-Out
- Travel Information
- Pharmaceutical and Medical Products
- Public Record and Publicly Available Information
- Access Requests by Public Authorities

The Foundation Needed for PIAs

- Policies *
- Procedures *
- Privacy Impact Assessments *
- Security Risk Assessments *
  - Both baked into your projects, repeatable
- Privacy Inventory *
  - Privacy Data Item of the Data Subject – Name, etc.
  - Where stored (applications)
  - Where stored (data center, country) and a whole lot more…
- Data Classification * Data Categories *
- Data Flow

An overview of the General Data Protection Regulation

- Data Flows *
  - Do you know where your sensitive data is?
  - Principle of Data Minimization
    - Spreadsheets?
- Data Protection by Design and by Default *
  - More on this later
- Key Security Principles that still apply *
  - Confidentiality
  - Integrity
  - Availability

An overview of the General Data Protection Regulation - Breaches

- The following link is utilized as a reference to review the GDPR regulation, which I obtained from ISC2: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG
- Now for Article 33 on breaches - **Notification of a personal data breach to the supervisory authority**

An overview of the General Data Protection Regulation - Breaches

- 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than **72 hours** after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the **supervisory authority** is not made **within 72 hours, it shall be accompanied by reasons for the delay.**
- **2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.**
- 3. The notification referred to in paragraph 1 shall at least:
- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach;
- (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

An overview of the General Data Protection Regulation - Breaches

- 4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
- 5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.
- Now, the concept of an internal breach….

An overview of the General Data Protection Regulation

- Concept of an Internal Breach
  - A bad process, not intentional, that allowed an unauthorized employee to see privacy data – caught the issue and no harm to the employee
  - No harm, no foul – in GDPR, this is a breach.
- Concept of Historic Breaches with respect to GDPR
- Phishing Training and Phishing your users, while maintaining and building trust
  - Train in security awareness and in how phishing works
  - Tell them they may be phished in next 10-30 days
    - If they report it, will earn points toward a prize
    - If they report an actual Phishing attack, more points…
  - Phish them
  - Reward the prizes
  - Repeat in an appropriate amount of time.

An overview of the General Data Protection Regulation 1/2

- **Supervisory authority – Article 51**
- 1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').
- 2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.
- 3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

An overview of the General Data Protection Regulation 2/2

- **Supervisory authority – Article 51**
- 4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

An overview of the General Data Protection Regulation

- Data Protection Officers
  - In Europe now
    - Some are contracted out
- Hired / Appointed by the Company
- Get very involved in the Policies, Procedures, and each of the controls, and in testing
- Get them involved early
- They report to the Data / Supervisory Authority
  - The company cannot fire them.
- Estimates range up to 28,000 plus new DPOs needed….

An overview of the General Data Protection Regulation

- Right to Erasure, Right to be Forgotten
  - Use case
    - Does everyone like this?
    - Is it the right thing to do?
      - Will it be the last word?
- **Enforcement May Differ Between Data Protection Authorities and Supervisory Authorities**
  - Spain
    - Fines go in the regulatory and enforcement body
    - Not all countries do this
      - Example of a concern I learned at a privacy conference early this year from a colleague at a large manufacturing co.
        - … One message across the entire company

An overview of the General Data Protection Regulation

- Two other items of Note:
  - Each Country can augment this regulation with rules of their own… while that may have started, I have not heard about that yet.
    - Some will be additional rules, some of it will be further explanation as required by the GDPR.
  - Case Law….
  - Also, regarding Brexit, it is my understanding that the UK will be under GDPR for about 5 months, until Brexit take effect.

An overview of the General Data Protection Regulation

- Now to talk about Privacy by Design and by Default, or Data Protection by Design and by Default
- Or PDB2
- Privacy Commissioner from province of Ontario in Canada, Dr. Ann Cavoukian

Data Protection Regulation Article 25 – PbD2

- **Requirements**
- The requirements, or constraints as they will be mandatory, as listed in Article 25, Data Protection by Design and by Default, of the GDPR are:
- 1. Taking into account the state of the art, the 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 posed by the processing, 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.
- 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
- 3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.
- (Note: Pseudonymization is the state where privacy data is no longer identifiable due to the use of an algorithm, or in combination with another set of data, stored separately, that allows for re-identification.

Data Protection Regulation Article 25

- **Interpretation of the Requirements**
- The following appears to be a valid interpretation of the requirements, from the standpoint of those subject to the regulation:
- We should identify the key data protection principles, which include data minimization, and the controls which meet them, and implement them based upon the results of the Privacy Impact Assessment.
- Essentially, we are being told to prevent a breach, whether we or our processor is involved.
- We will monitor and demonstrate compliance, either internally or with external assistance.

Data Protection Regulation – Data Privacy Principles

- **Some Key Principles to Implement, Maintain, and Demonstrate in Providing Data Protection**
- Here are several relevant principles that should be implemented with appropriate controls, and monitored for effectiveness in achieving proper security, privacy, and compliance:
- *Data Minimization* – this is closely related with knowing where your data is, particularly your sensitive privacy data, and purposely minimizing the data itself, and its use. A Privacy Inventory is needed to achieve data minimization. Among other data elements contained, it should identify the systems in which data privacy elements are present and maintained.
- *Purpose Limitation* – proper design elements, and reviews of the design, are needed to ensure that the original intent has not been expanded. If that intent is expanded, beyond which you have received consent from the data subject, you could be subject to fines.
- *Transparency in processing* – Tell the data subjects how you will collect, process, store, and report their data, and conduct reviews, to ensure that you the Controller and your Processor(s), do just that.
- The following three principles are not new to you, but I would argue that they have increased responsibility with the impending GDPR:
- *Confidentiality* – Keeping data subjects' privacy data confidential to only those with a need to know.
- *Data integrity* – Ensuring data subjects' privacy data is not inappropriately modified.
- *Availability* – Ensuring privacy data and the systems that process it are available.

Data Protection Regulation

- The Foundation You Need in Place for this…
  - Policies
  - Procedures
  - Privacy Impact Assessments
  - Security Risk Assessments
  - Privacy Inventory
  - Data Flows
  - Data Privacy Categories
    - And what you literally should be doing for your privacy data with or without GDPR… but again, this also is a culture change….

Data Protection Regulation

- Other References
  - Privacy by Design and by Default
  - Data Privacy Life Cycle
  - NIST Privacy Engineering

What a Processor is, and Controls Needed for your Processors.

- Controller
- Processor
- Controls
  - Categories of Privacy Data
  - Risks
  - Controls
  - Contracts
  - Compliance methodology

The Challenges Around Cloud Computing

- Controls
  - Killing Cloud Quickly, an article…
  - Categories of Privacy Data
  - Risks
  - Controls
  - Contracts
  - Incidents, notification of a breach
  - Compliance methodology
  - NIST and the Audit Language plan
  - CASBs, and other tools will be of great use here; one of the vendors has a good framework from Gartner
    - However, we will have to risk assess those tools as they monitor workforce members' behavior….

The Need to Demonstrate Compliance Upon Demand

- Compliance, demonstrate compliance upon demand, and certification
- The compliance portion is going to be key – automate this as much as possible, but work into that….
- Data Protection Authority and Supervisory Authority
- Spain's Data Protection Authority – may be your Supervisory Authority
- A large manufacturing company's concern
- One Message, Everywhere! (But back it up!)
- How hard is it to get compliance upon demand?
- Certification

Wrap up and Next Steps

- We've covered a lot today…
- Assessment of where you are with respect to the needed controls
- Define a program, prioritized by project
- Seek additional funding for this year if needed
- Areas to Strengthen
  - Incident Response Plan
    - Scenarios
    - OODA Loop – Observe, Orient, Decide, Act
      - Fighter Pilot developed it – building into IR Phases
  - DR/BCP
    - DRII Professional Practices
    - RTO, RPO – Requirements defined by BIA – feeds IRP
  - Then there is your Supply Chain…

Questions??

Thank you Very Much,

Harvey