RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: GRC-R02

THE GDPR IS ONLY FOR EUROPE – RIGHT?

Lawrence D. Dietz, Esq.

General Counsel & Managing Director, Information Security
@Colonel_Larry

Why You Need to Pay Attention to GDPR

Financial Reasons

- You may have to comply with GDPR
  - Extended Reach
    - EU Citizens Wherever They May Reside
    - Doing business with the EU
- Fines are very substantial:
  - Up to 4% Annual Revenue or €20 Million
- Your multinational customers will make you comply to do business with them.

It’s the right thing to do.

- Proper Intent
  - Give individuals more control over their personal data.
  - Mitigate the risk of harm due to a breach.
- Others are relying on GDPR as a standard:
  - Investors
  - Customers
  - Other Nations

Universal Principles

- Lawfulness, Fairness & Transparency
- Limitation of Purpose
  - Specified, explicit & legitimate
- Data Minimization
  - Adequate, relevant and limited
- Accuracy
- Storage Limitation
  - Only as long as necessary for the purpose.
- Integrity & Confidentiality
  - Appropriate technical & organizational security measures.
- Accountability

ILLUSTRATIVE SCENARIOS – MINI CASE STUDIES

Disclaimer

- These are fictional vignettes designed to encourage discussion and raise issues where the GDPR may be relevant.
- This session is not intended to be legal advice which can only be obtained from licensed counsel with whom you have a relationship.
- Creativity is encouraged.

Scenario 1

- You work for a company that does business in many countries around the world. At the moment you do not have any offices in non-English speaking countries.
- The CEO's favorite niece is on an assignment as an intern in the marketing department. Since she is majoring in Italian she wants to design a website in Italian.
- Will you have to comply with GDPR?

Scenario 2

- Sally Salesperson collects a dozen business cards from a conference in Rome.
- She immediately puts all the contact information into the corporate sales data base.
- What questions would you have to ask in order to determine if GDPR applies?

Scenario 3

- You work for Super Spuds in Pocatello, ID. Your company is very small, but it is famous for its specialty equipment used in potato farming.
- Would any of the following trigger GDPR?
  - Hiring an answering service or opening an office in:
    - Paris
    - Zurich
    - Dublin

Scenario 4

Big Tech Co is working on a major product launch. To ensure global appeal they temporarily transfer several employees from Europe to work on the project in the Corporate HQ in the United States.

1. Does this mean that BTC must comply with GDPR?
2. What if all the employees being transferred are American citizens?

Scenario 5

- One of your former employees has moved to Germany. His performance was a bit sub-standard, but he was not fired.
- After he is settled in Germany, he demands that you delete all of the information you have in his personnel file?

1. Are you compelled to do so?
2. What if he is an American citizen – does that change your answer?

Scenario 6

- Tiny Tidbit (TT) in Santa Cruz, CA produces gluten free, vegan snacks. They employ 10 people. The are negotiating with Daunting Distributors (DD) to carry their product worldwide.
- DD is a multi-national with HQ in Montreal, Canada. DD wants TT to sign a complicated contract containing terms and conditions to comply with the GDPR.
  - Does TT have to agree to those terms?
  - What if DD wants TT to translate their website and marketing materials into French because that is the law in Canada.
    - Does this sound any alarm bells?

Scenario 7

- Gerry is a German Citizen who is an engineer employed by Large Lens Co in Munich.
- The New Jersey manufacturing and assembly plant wants Gerry to help them with a 90 day project.
- He arrives with his company laptop, personal iPad, a company iPhone and a personal iPhone.
  - What potential GDPR issues are there?

Scenario 8

- You are a newly hired CISO for Padlock Insurance company at their HQ in Chicago. Your boss, the CFO, is also relatively new.
- He stops you in the hall at 6 PM and asks “Hey, with SOX, HIPAA, HiTech, etc. do we really need to worry about GDPR?”
- He continues “Please give me 3 bullet points to take to the CEO tomorrow at 9 AM before his 10 AM Board meeting.”

Scenario 9

- You work for a company that manufacturers paper towels and toilet paper.
- You are asked to lead a team to implement a new digital marketing system designed to provide more detailed information about customers and prospects.
  1. Are you compelled to perform a Data Privacy Impact Analysis?
  2. Should you consider adopting a ‘privacy by design’ philosophy or just look for the lowest cost options?

Scenario 10

- You work for a chain of hospitals.
- You are asked to lead a team to implement a new patient and medication system.
  1. Are you compelled to perform a Data Privacy Impact Analysis?
  2. Should you consider adopting a ‘privacy by design’ philosophy or just look for the lowest cost options?

Applying What You Have Learned Today – Part 1: Next Week

- Form a Project Task Force With Clear Roles & Responsibilities
  - Include: An Executive Sponsor and CFO, CIO, CISO, Legal & HR representation.
- Establish Data/Application Inventory Teams
- Determine if your organization has every performed a Data Audit
- Update subcontract, supplier, temporary employ and other appropriate contracts to include terms and conditions to comply with and implement GDPR principles.

Applying What You Have Learned Today – Part 2: Next 60 Days

- Initiate a Data Mapping and Inventory Project across the organization.
- Determine the nature and extent of data transfers in and out of the EU.
- Develop a project plan to initiate or improve data auditing to include:
  - Validation of Data Subject Consent (Opt in or exemption)
  - Source of Data
  - Confirmation of legitimate use and data storage limitations
  - Assess the nature of data sharing to include application and geography

Applying What You Have Learned Today – Part 2: Next 6 Months

- Review, revise and test breach notification procedures.
- Design and conduct a Table Top Exercise to test your breach discovery and notification process.
- Plan for an annual breach simulation exercise in 90 days.

Thank You – Q & A

Lawrence D. Dietz, Esq.

LDietz@talglobal.net

TALGLOBAL
INTEGRITY • RELIABILITY • CONFIDENTIALITY