



# GENERAL DATA PROTECTION REGULATION (GDPR)

Stan Hess – April 2018



# STAN HESS

- Chief Technology Officer for a global professional services firm
- Writer and owner of College360, an education accreditation tool and management system
- Over 20 years in global IT and financial management

- Project Management Professional (PMP)
- Certified Information Security Auditor (CISA)
- Certified in Risk in Information Systems Control (CRISC)
- Cisco Certified Network and Design Associate (CCNA / CCDA)
- Microsoft Certified Systems Engineer (MCSE)
- ITIL Certified

# WHAT IS GDPR?

- GDPR is the European Union's upcoming General Data Protection Regulation
- It was approved on April 14, 2016
- It goes into effect, for compliance, on May 25, 2018
- It replaces the 1995 EU Data Protection Directive

# 1995 EU DATA PROTECTION DIRECTIVE

- GDPR is the European Union's upcoming General Data Protection Regulation
- It was approved on April 14, 2016
- It goes into effect, for compliance, on May 25, 2018
- It replaces the 1995 EU Data Protection Directive

# WHO DOES GDPR APPLY TO?

- Any company that handles any personally identifiable information (PII) on any EU citizen

The EU classes personal data as “**Any information relating to an identified or identifiable natural person,**”

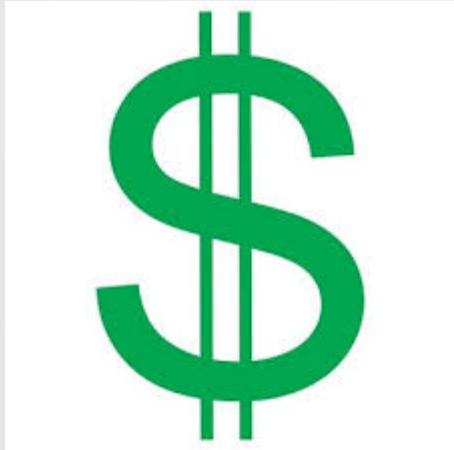
## PII

- Personally Identifiable Information
- US: Information that can be used independently OR with other information to identify, contact or locate an individual
- NIST: “Any information about an individual maintained by an
- EU: There is no concept of PII. It’s simply “personal data” meaning potentially a much broader scope

# PERSONALLY IDENTIFIABLE INFORMATION

- **US:** Information that can be used independently OR with other information to identify, contact or locate an individual
- **NIST:** “ Any information about an individual maintained by an agency” including
  - Any information that can distinguish or trace an identity such as a name, social security number, date / place of birth, maiden name, biometrics, etc.
  - Any information linkable to an individual such as medical, *educational*, financial or employment data
- **EU:** There is no concept of PII. It’s simply “ personal data ” meaning potentially a much broader scope

# WHY SHOULD I CARE?



- Fines of up to \$20M Euros
- or
- 4% of total annual revenue

*whichever is greater..*

# ROLES AND DEFINITIONS

- Data Controllers
  - Entities or individuals that need to process personal data to do business
- Data Processors
  - Process personal data on behalf of the controller



# PREPARATION

- I. Awareness
  - I. Communication and Transparency
  
- II. Data Inventory and Categorization
  - I. What do I have?
  - II. Where did it come from?
  - III. Who do I share it with?
  
- III. Communication
  - I. Review your current privacy notices
  - II. Assess and re-communicate

# PREPARATION

## IV. Rights

- I. Check your processes, procedures and documentation to verify individuals rights
- II. How will you retain or delete data?
- III. What formats will you use and where is it stored?

## V. Access Requests

- I. How will you handle requests to access data?

## VI. Legality

- I. Review and validate your legal basis for handling or processing data

# PREPARATION

## VII. Consent

VII. Review how you seek, obtain and record consent for sharing your data

## VIII. Age

VII. Are you bound by any specific age regulations?  
Children?

## IX. Data Breaches

VII. Do you have a defined and tested process and policy on data breaches?

VIII. Do you have any detection methods in place?

# PREPARATION

## X. GDPR

- X. Familiarize yourself with GDPR

- XI. Stay engaged

## XI. Roles and Responsibilities

- X. Assign someone accountability for data protection and compliance

## XII. Jurisdiction

- X. Do you have other jurisdictions you operate under?

- XI. National, Regional, Local?

# QUESTIONS