Data Inventories: GDPR as a Forcing Function

MTUG WEBINAR

APRIL 11, 2018

DEER BROOK
Information Security . Privacy . Technology

Introduction to Deer Brook

Ande Smith, President

- Former Director of Information Security, Delhaize America
- Attorney since 1997, practicing in IT and compliance both in-house and private practice
- Established Deer Brook in 2012 after serving as Tilson Technology COO and IS consulting
  - Numerous data breach and cyber advisory clients over the past 5 years
  - Founding member, Maine Cyber Security Cluster; Cyber Evaluator, NLE-12; Featured speaker at NE ISACA conferences, etc.
- Former submarine officer; retired from the US Navy Reserve as a Captain

Deer Brook Team

- Core team of technical resources, with industry certifications, including CIPP/CISSP/CISA
- EnCase forensic lab partner
- Data-breach experienced communications specialist

What is the GDPR

- Stands for “General Protection of Data Regulation”
- Basic Idea: European Union has established a new, higher set of protections for the privacy of EU citizens. Principals include the right to anonymity.
- Set of Rules set to take effect May 2018.
- Applicability: Organizations that offer goods/services to EU citizens, no matter where located
- Key Elements:
  - Enhanced Personal Privacy Rights
  - Increased Duty for Protecting Data
  - Mandatory Data Breach Reporting
  - Significant Penalties for Non-compliance

Who are you: Processor or Controller?

Different GDPR requirements and obligations apply whether you're a controller or processor

- Controller is a person or organization that determines the purpose and means of processing personal data
- Process is a person or organization that processes data on behalf of the controller.

Controller Obligations

- Responsible for meeting privacy principals, including by downstream processors
- Principals include lawfulness, fairness and transparency, data minimization, accuracy, storage limitation and integrity, and confidentiality of personal data

Processor Obligations

- Must be able to implement controls sufficient to meet the obligations of the GDPR

Implications for Data Inventories

Right to be Forgotten

- Person has the right to request the controller to erase his or her personal data without undue delay where: the data is no longer necessary for the purposes collected; the data subject withdraws consent; or the data subject objects to data processing
- Where the controller has made the data public, the it shall take reasonable steps to inform the controller processing that data of the erasure request

Consent

- Must be freely given, specific, informed, and unambiguous indication of the person's wishes
- For special categories of personal data, explicit consent is required
- Persons have the right to object to processing unless the controller demonstrates compelling legitimate grounds for processing (e.g., law enforcement)
- Where personal data is processed for direct-marketing, persons have the right to object at any time to the processing
- Data subjects have the right not to be subject to a decision based solely on automated processing — including profiling — unless the data subject has given explicit consent, or where the processing is authorized by contract or in HIPAA/HITECH, GLB/FFIEC, FERPA, etc.

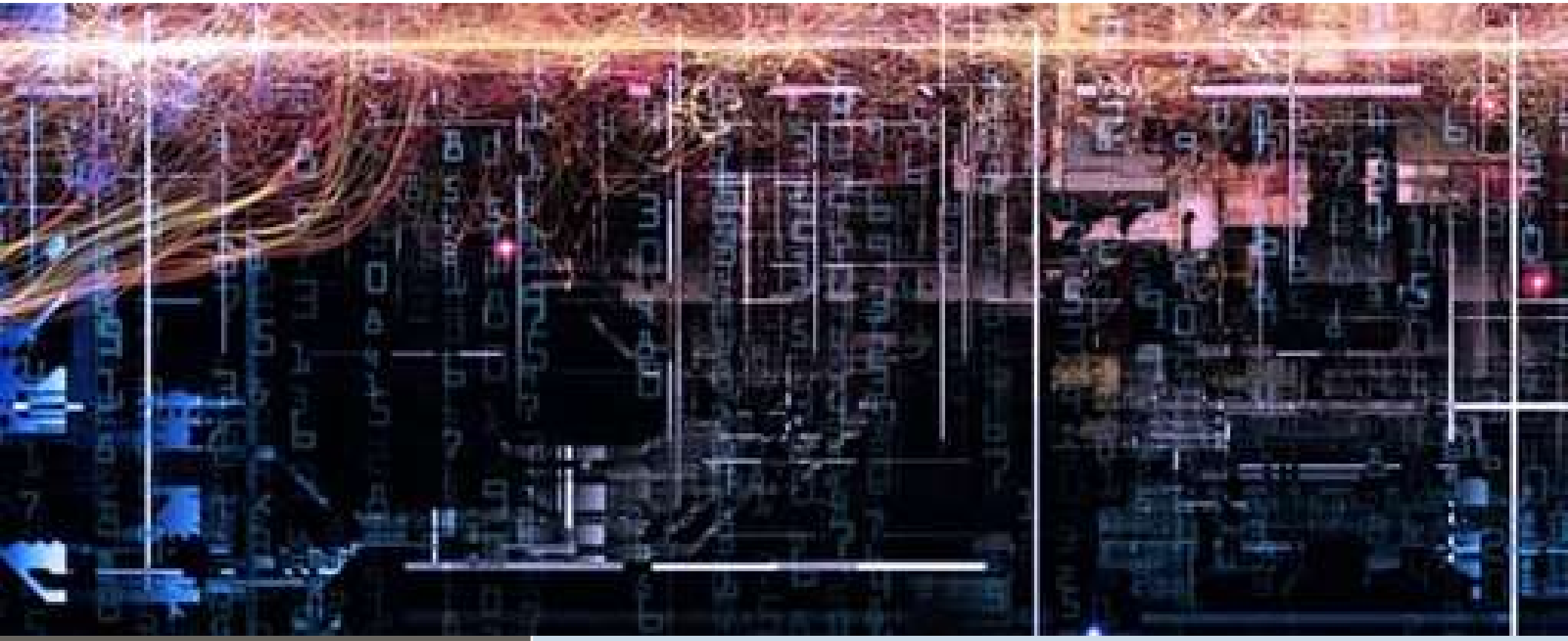
Likely Challenges

Defining what you must protect
- First must discover what you have;
- Likely will require data classification to manage what's regulated and what isn't

Data Governance
- Time for another program!
- Generate notice of how data is collected, used and processed
- Ability to discontinue processing that user's data
- Handle request for correction , erasure and transfer of data
- Provide user with a copy of their data
- Temporary processing halts
- Data Protection Impact Assessments

Data Protection
- Probably requires revisits to architecture and controls, especially for "by-default" control application
- CIA attributes must all be examined and meet "high standards" – de facto encryption
- Detailed breach response; 72 hour notification generally

Audit
- Consent Tracking
- Flows to/from EU
- 3rd Party xfers



DEER BROOK

Information Security . Privacy . Technology

Questions and Discussion

Ande Smith, President

asmith@deer-brook.com | +1 207.712.1350 | deer-brook.com