Compliance Strategies for the New European General Data Protection Regulation

October 18, 2017

David Vance Lucas
General Data Protection Regulation (GDPR)

- Designed to update and harmonize European Union (EU) data privacy laws
- Replaces the EU Data Protection Directive 95/46/EC
- Was approved by the EU Parliament in 2016
- Enforcement begins **May 25, 2018** – including application of heavy fines
GDPR Legislation History

- **1995** – European Commission adopts Data Protection Directive to regulate processing of personal data
- **2012** – European Commission proposes updating data protection regulations
- **2015** – Council of the European Union approved GDPR for legislative “Trilogue” process
- **2015** – Parliament and Council approve GDPR
- **January 2016** - Signing of the new GDPR
- **April 2016** - GDPR adopted by the Council of the European Union
- **April 2016** - GDPR adopted by the European Parliament
GDPR Force and Effect

- **May 2016** – GDPR goes into effect 20 days after being published in the EU Official Journal, but with a 2 year grace period

- **May 25, 2018** - 2 year grace period will expire and the GDPR will become fully enforceable throughout the EU

- Organizations not in compliance will face heavy fines
GDPR General Intent

GDPR is intended to:

- Protect EU citizens’ data privacy rights
- Regulate organizational data privacy practices
- Protect EU citizens’ privacy and mitigate data breach injuries
- Reflect realities of current data-driven world vs. the 1995 Directive
GDPR Definition of Personal Data

“Personal data” means any information relating to an identified or identifiable natural person (Data Subject);

an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier

or, to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
GDPR Key Provisions

Extraterritorial - Greatly expands jurisdiction

- Applies to companies processing personal data of data subjects residing in the EU - **regardless of company’s location**

- Applies to the processing of personal data by controllers and processors in the EU, **regardless of whether the processing takes place in the EU**

- **Non-EU businesses** processing the data of EU citizens will **have to appoint a representative** in the EU
GDPR Key Provisions

Penalties

- Fines can be up to 4% of annual global turnover (revenue), or €20 Million - whichever is greater

- Tiered fines
  - Can be fined 2% for not having their records in order (article 28)
  - Can be fined 2% for not notifying the supervising authority
  - Can be fined 2% for not informing data subject about a breach or not conducting impact assessment

- Fines apply to controllers and processors -- ‘clouds’ will not be exempt from enforcement
GDPR Key Provisions

Consent

Increased requirements for consent

- Request for consent must be given in easily accessible form
- Companies cannot use long illegible legalese
- Purpose for data processing must be included with the consent
- Must be as easy to withdraw consent as it is to give it

Consent must be distinguishable, clear and plain language – think UCC Disclaimers
GDPR Key Provisions

Breach Notification

- Breach **notification is mandatory** where a data breach is likely to “**result in a risk for the rights and freedoms** of individuals”

- **Notification** must be done **within 72 hours** of becoming aware of the breach
GDPR Key Provisions

Right to Access

Expanded rights of Data Subjects

- Data subjects have **right to obtain details** from data controller regarding processing of personal data, and **where and for what purpose**

- Controller is **obligated to provide a copy** of the personal data, free of charge, **in an electronic format**
GDPR Key Provisions

Data Portability

GDPR introduces data portability

- Data Subject has right to receive their Personal Data
- Data Subject must be provided data in a ‘commonly used and machine readable format’,
- Data Subject has the right to transmit data to another controller
GDPR Key Provisions

Right to be Forgotten

Data Erasure -- the right to be forgotten

- Data Subject is entitled to have the data controller erase Personal Data
- Cease further dissemination of the data
- Have third parties halt processing of the data
GDPR Key Provisions

Data Protection Officers

DPO is mandatory for controllers and processors whose core activities:

- Processing operations which require regular and systematic monitoring of Data Subjects on a large scale

- Special categories of data or data relating to criminal convictions and offenses.
GDPR Key Provisions

Data Protection Officers

- Appointed based on professional capabilities - expert knowledge of data protection laws and practices
- May be an employee or external provider
- Contact information must be provided to relevant DPA
- Must be provided with appropriate resources and maintain expert knowledge
- Must report directly to the highest level of management
- Must not be responsible for other tasks that could result in a conflict of interest
GDPR Organizational Summary

Chapter 1: General Provisions - Subject matter, objectives, scope and territorial scope

Chapter 2: Principles - Personal data processing, categories of personal data and consent

Chapter 3: Rights of the Data Subject – Transparency, Access, Rectification and Erasure

Chapter 4: Controller and Processor - Data protection design, Records, Security, Notifications of breach, impact assessment, data protection officers, Codes of Conduct, certification and Monitoring
GDPR Organizational Summary

Chapter 5: Transfer of personal data to third countries of international organizations – Transfers, safeguards and International cooperation

Chapter 6: Independent Supervisory Authorities - Supervisory Authority

Chapter 7: Co-operation and Consistency - Cooperation of supervisory authorities and European Data Protection Board
Chapter 8: Remedies, Liability, and Sanctions – Complaints, judicial remedies, and administrative fines and penalties

Chapter 9: Provisions relating to specific data processing situations - Public access to official documents, obligations of secrecy and data protection rules of churches and religious associations

Chapter 10: Delegated Acts and Implementing Acts - Exercise delegation and Committee procedure

Chapter 11: Final provisions - Repeal of Directive 95/46/EC
EU GDPR Resources

http://www.eugdpr.org/more-resources-1.html
US DoD and DSS Equivalents

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7000 et. seq.

- DFARS regulations adopted October 2016
- Compliance deadline December 31, 2017

Defense Security Services “insider threat program” (ITP)

- May 2016 “insider threat program” (ITP)
- NISPOM Change 2 required the implementation, certification and maintenance of an ITP
Scope of New DFARS and DSS ITP

Protecting national security data and networks from cybersecurity threats

- Government contractors and subcontractors that handle “controlled unclassified information”
- Defense information on systems that support the performance of DoD contracts
- Covered information systems must comply with the security requirements in NIST CUI
- Covered information systems are subject to the security requirements in NIST Special Publication (SP) 800-171
Similarities Between GDPR and New DFARS / ITP

- Must report cyber incident within 72 hours of discovery (DFARS 252.204-7012)
- Must send malicious software to the DOD Cyber Crime Center (DFARS 252.204-7012subsection (d))
- Obligated to preserve copy of system and monitoring data for 90 days from an incident report, and allow DOD access for forensic analysis (DFARS 252.204-7012 subsections (e)-(f))
- Requires appointment of an Insider Threat Program Senior Official (ITPSO) (NISPOM Change 2)
- Requires awareness training of cleared personnel by May 31, 2017 (NISPOM Change 2)
GDPR Compliance Strategies

- Assessment
- Risk mitigation and response
- Operational compliance
GDPR Compliance Strategies

Assessment

Operational considerations – Personal Data Rights Provisions
- Employment and Employee Benefits Agreements
- Employee Proprietary Rights Agreements
- Employee Handbook and Code of Conduct
- Non-disclosure and Confidentiality Agreements
- Customer Agreements
- Teaming, Secondment and Joint Development Agreements

Procedures for tracking Personal Data and Consents

Physical and cyber security of Personal Data
GDPR Compliance Strategies

Policies and Procedures

Advanced preparations

- Evaluation of need for Personal Data
- Identification of Personal Data, uses and locations
- Assessment of possible physical, cyber and data weaknesses
- Advanced understanding of business, operations, customers and employees
- Determine need for DPO and EU Representative

Rapid response planning

- Analysis of possible response strategies
- Identification of jurisdictions which could be involved
- Analysis of probable damages and mitigation plans
- Pre-determination of resources for rapid response
GDPR Compliance Strategies

Implementation

Advanced preparation checklist:

- Description of Personal Data in possession
- Accurate contact information for customers and employees in the event of a breach
- Compliant Policies, Protections and Procedures
- Prepare training of employees and contractors
- Implement required EU Safeguards for export of Data
- Pre-modeling of possible mitigation plans
- Summaries of jurisdictions and related legal information
- Pre-determination of appropriate response resources
DFARS / ITP Compliance Strategies

Assessment

Review systems

Perform security risk assessments
DFARs / ITP Compliance Strategies

Preparation checklist:

- Evaluate systems and facility security
- Assess preparations and protections
- Review policies and procedures
- Evaluate employee training and resources
- Develop rapid response capability to Data and Network threats and breaches
- Develop procedures for incident response, document retention, audits, awareness and training
DFARs / ITP Compliance Strategies

Implementation - December 31, 2017 deadline

Assess and implement

- Compliant policies and procedures
- Access control, authentication, media protection, physical protection, monitoring, and malware defense as specified in NIST SP 800-171
- Pre-determination of IT, legal and accounting resources for rapid response and compliance
- DFARS Incident response plan for reduced notice period
Additional information is available at:

http://www.dss.mil/it/index.html
QUESTIONS?

For more information contact:

David Vance Lucas
Bradley Arant Boult Cummings, LLP
256-517-5131
dlucas@bradley.com