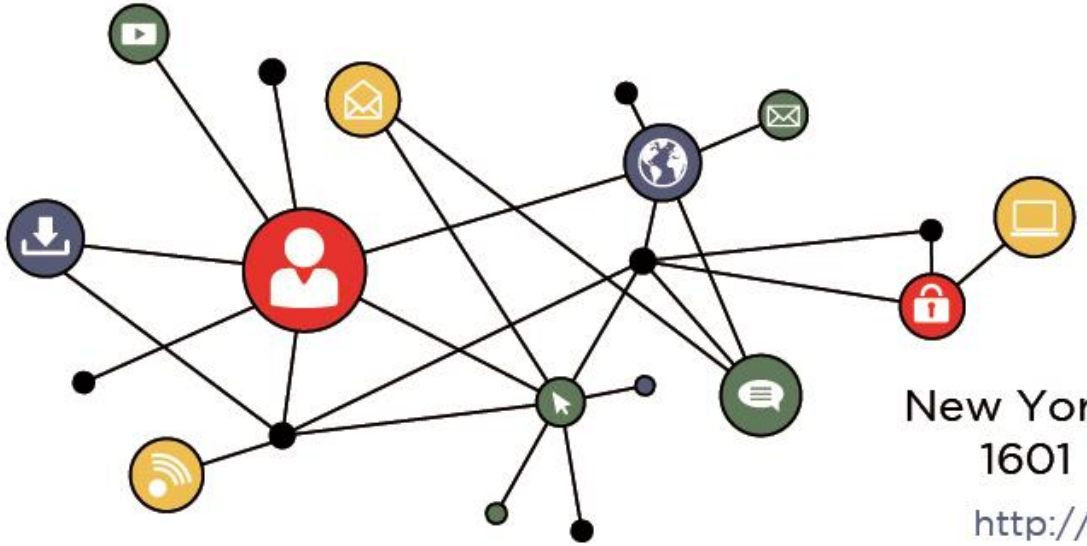
ARMA INTERNATIONAL

ARMA METRO NYC ANNUAL SPRING CONFERENCE

RIM & IG for Today & Tomorrow



TUESDAY, MARCH 7, 2017

8:00 am – 5:00 pm with
Reception immediately following

New York Executive Conference Center
1601 Broadway, New York, NY 10019

http://armanyc.org/2017_Spring_Conference

WHAT GDPR MEANS FOR RECORDS MANAGEMENT

Presented by: Sabrina Guenther Frigo

Overview

Background

Basic Principles

Scope

Lawful Processing

Data Subjects' Rights

Accountability & Governance

Data Transfers

Enforcement, Remedies & Penalties

Takeaways & Questions

BACKGROUND & BASIC PRINCIPLES

Background

General Data Protection Regulation (GDPR)

- Replaces Data Protection Directive 95/46/EC
- Broader scope, more stringent and more detailed requirements, and higher penalties
- Some activities subject to additional Member State requirements
- Comes into force on May 25, 2018

Basic Principles

- Transparency, lawfulness, and fairness
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Security
- Accountability

GDPR SCOPE

Territorial Scope

GDPR applies to:

- Organizations established in the EU
- Organizations **outside** of the EU that offer goods and services to EU citizens
- Organizations **outside** of the EU that monitor EU citizens' behavior in the EU (i.e., track online behavior)
- See Regulation (EU) 2016/679, Article 3

Scope – Data Controllers & Data Processors

GDPR will apply to both “data controllers” and “data processors”

- Data processors will be required to maintain records of personal data and processing activities and will be subject to greater liability if responsible for a breach
- Data controllers cannot push liability onto processors—must ensure contracts require processors to comply with GDPR

Scope – Personal Data

Personal Data

- "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…" (Article 4(1))
  - Examples: "name, an identification number, location data, an online identifier"
- Includes pseudonymized data but not anonymous data (Article 4(5))

Scope – Special Categories of Personal Data

Sensitive personal data subject to heightened protections (Article 9)

- Includes:
  - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership,
  - genetic or biometric data processed to uniquely identify someone,
  - data concerning health or sex life/sexual orientation

LAWFUL PROCESSING

Lawful Processing

Must have a legal basis for processing personal data:

- With consent
- When necessary
  - To perform, or enter into, contract with data subject
  - Comply with a legal obligation
  - To protect vital interests of data subject or another person
  - For the performance of a task carried out in public interest
  - For legitimate interests pursued by the controller or third party, except when such interests are overridden by the interests or rights of the data subject

Lawful Processing - Consent

Consent requires some “clear affirmative action” (Articles 4(11), 7)

- Silence, pre-checked boxes, or inactivity will not constitute “consent”
- Data subject must be given right to withdraw consent at any time and must be informed of this right before giving consent
- Data controller must **maintain a record** regarding how and when consent was given

Lawful Processing – Direct Marketing

Direct marketing included in “legitimate interests” ground for processing

- BUT data subject must be given right to object at any time to use of personal data for direct marketing or for profiling related to such marketing
- Must present this right clearly and separately to the data subject at time of first communication

DATA SUBJECTS' RIGHTS

Data Subjects' Rights (Chapter III)

- Be informed (notice)
- Access personal data
- Correct personal data
- Erase personal data
- Data portability
- Restrict processing
- Object to processing
- Restrict automated decision making and profiling

Right to Be Informed (Notice)

Numerous requirements for contents of notices to data subjects (Articles 13-14)

- Controller's representative/DPO contact
- **Purpose of and legal basis for processing**
- Categories of personal data
- Sharing/transfers
- Source of personal data (if not data subject)
- **Retention period(s) for personal data**
- Existence of data subjects' rights
- Consequences of failure to provide
- Automatic decision making

Rights to Access, Correct Personal Data

Individuals may access personal data organizations have about them and correct incomplete or inaccurate information (Articles 15-16)

- Must respond to requests within 1 month, or 3 months for complex request
- Must inform (1) third parties to whom data have been disclosed of correction and (2) individuals that their data have been disclosed to third parties

Right to Erasure ("Right to be Forgotten")

Must erase data and prevent processing in certain circumstances and at individual's request (Article 17)

- Data no longer necessary for original purpose for which it was collected
- Individual withdraws consent
- Individual objects to further processing and no overriding "legitimate interest" to continue processing
- Data are unlawfully processed
- Erasure necessary to comply with legal obligation
- Data related to offer of "information society services" (e.g., online platforms) to a child

Right to Erasure (cont.)

- If controller has made data public, must take “reasonable steps,” given technology and cost of implementation, to inform other controllers that the individual has requested erasure
- If controller has disclosed data to third parties, must notify those third parties, unless impossible or would involve disproportionate effort
- Some limited exemptions from compliance (e.g., to exercise right of freedom to expression and information)

Right to Data Portability

Gives individuals the right to obtain and reuse their personal data easily on different services (Article 20)

- Applies (1) to personal data the individual provides to the controller when processing is (2) based on consent or performance of a contract and (3) carried out by automated means (no paper records)
- Requires controller to provide data in structured, commonly used, and machine-readable format

Right to Restrict Processing

Individuals can request controller stop processing their personal data when: (Article 18)

- Individual contests accuracy of personal data
- Individual objects to further processing and controller determining whether overriding “legitimate interest” exists to continue processing
- Data are unlawfully processed
- Controller no longer needs the data, but the individual needs the data to establish or defend a legal claim

Right to Object to Processing

Individuals can request controller stop processing their personal data when: (Article 21)

- Used for direct marketing, including profiling
- Processed based on controller's "legitimate interests" or public interests/exercise of official authority
- Processed for research and statistics

Rights Related to Automated Decision Making

Individuals have the right not to be subject to decisions based solely on automated processing if the decisions produce legal effects or a “similarly significant effect” on the individual (Article 22)

- Examples: online credit decisions, e-recruiting, employment
- Profiling and automated decision making may be used if the individual consents, it is necessary to enter into or perform a contract, or it is authorized by EU or Member State law

Individual Rights & RIM

- Numerous individual rights require different systems, functionalities
- May generate new types of records
- Potential need to demonstrate compliance
- Increasing focus and impact on retention

Accountability & Governance

Data Protection by Design and by Default

- Data protection by design integrates data protection into business processes through “appropriate technical and organisational measures, such as pseudonymization … .” (Article 25)
- Data protection by default relies on those measures to limit processing of personal data “without the individual’s intervention” (Article 25)
- EU may develop codes of conduct and certification schemes to help companies meet these obligations

Data Protection Impact Assessments (DPIAs)

Controllers must undertake DPIAs when a new type of processing is “likely to result in a high risk to the rights and freedoms”(Article 35)

- Examples: processing sensitive data “on a large scale”, “systematic and extensive” automated decision making
- Supervisory Authorities expected to publish other examples of processing that require DPIAs

Contracting with Service Providers

GDPR imposes numerous requirements for contracts with service providers (i.e., "processors") (Article 28)

- Contracts must be in writing and must include obligations regarding breach, audits, etc.
- Obligations flow down service provider chain
- EC and Supervisory Authorities may publish standard service provider contract clauses

Records of Processing Activities - Controllers

Controllers must keep written records related to personal data processing (Article 30)

- Contact for controller, representative and DPO
- Purposes of processing
- Categories of personal data and data subjects
- Recipients of personal data when shared
- Transfers of personal data to third countries or international organizations and the documentation supporting transfer
- **Retention period(s) for personal data “where possible”**
- General description of security measures “where possible”

Records of Processing Activities - Processors

Processors also must keep written records related to personal data processing (Article 30)

- Contact for processor and controllers and their representatives and DPOs
- Categories of processing
- Transfers of personal data to third countries or international organizations and the documentation supporting transfer
- General description of security measures “where possible”

Data Security & Breach Notification

- Controllers and processors must implement appropriate technical and organizational security measures (Article 32)
- Controllers must notify supervisory authority of personal data breach “not later than 72 hours after having become aware of it” (Article 33)
  - Processors must notify controllers of breach “without undue delay”
- Controllers must document personal data breaches to demonstrate compliance

DPOs & Representatives

- Companies outside the EU that are subject to GDPR must designate in writing a representative in the EU (Article 27)
- Certain controllers must appoint a Data Protection Officer (if core activity involves regular monitoring on a large scale or large scale processing of sensitive data) (Article 37)

Role of RIM

- Explicit recordkeeping requirements
- Increasing complexity of other records generated
- Importance of records for accountability

DATA TRANSFERS

Data Transfers (Chapter V)

Transfers of personal data out of the EU restricted unless:

- “Adequacy” determinations (includes Privacy Shield)
- Binding Corporate Rules
- Standard Contractual Clauses
- Code of conduct approved by supervisory authority (new)
- Certification under approved certification mechanism (new)
- Derogations (includes explicit consent) (Article 49)

ENFORCEMENT, REMEDIES & PENALTIES

Enforcement

Supervisory Authorities (DPAs) have extensive authority, subject to judicial review:

- Monitoring and enforcing compliance with the GDPR
- Conducting investigations (requests for information, audits)
- Issuing warnings
- Imposing fines
- Banning processing and cross-border data transfers

Remedies & Penalties

- Individuals may lodge complaints against controllers and processors and be compensated for damage resulting from non-compliance
- Fines are discretionary and must be imposed on case-by-case basis. There are two tiers of fines:
  - Up to € 10 million, or 2% of annual global turnover, whichever is higher, and
  - Up to € 20 million, or 4% of annual turnover, whichever is higher

TAKEAWAYS & QUESTIONS

Takeaways

- GDPR is expansive and complex, and the stakes are high
- GDPR guidance and compliance plans continue to evolve, but it **will** affect RIM
- You can help!

QUESTIONS?