Cloud Security Alliance
Legal Information Center
San Francisco, April 20, 2015

Data Protection in the European Union What's Next?

Francoise Gilbert
Managing Attorney
IT Law Group

IT Law Group

Francoise Gilbert

- Founder & Managing Attorney, *IT Law Group*, Palo Alto
- Information Privacy & Security, Cloud Computing specialist
- Author & Editor, *Global Privacy & Security Law* (2 volumes, 3,600 pages, 68 countries) (Wolters Kluwer Publishing)
- Founding Member & General Counsel of the *Cloud Security Alliance*
- CIPP/US; CIPM
- Admitted to practice law in CA, IL and France

IT Law Group

- Niche law firm that focuses on information privacy and security, data governance and cloud computing
- Providing services to clients in the US and throughout the world through long term relationships with carefully selected privacy / security lawyers established on all continents

Current Trends in the EU

- **Cloud Computing**
  - Opinion WP 196 (July 2012)
- **Big Data**
  - Opinion WP 221 (September 2014)
- **Internet of Things**
  - Opinion WP 223 (September 2014)
- **Right to be Forgotten**
  - Guidelines WP 225 (November 2014)
- **Procedure of Issuing Common Opinion on Contractual Clauses**
  - WP 226 November 2014)
- **Data protection reform**
  - Opinion WP 191 (March 2012)

European Union Privacy 2.0

- *General Data Protection Regulation*
  - *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*
  - Intended to replace Directive 95/46/EC
- *Directive on the protection of individuals with respect to the processing of personal data for prevention, investigation, detection, prosecution of criminal offenses*
  - *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf*
  - Intended to replace Framework Decision 2008/977/JHA

Status = In progress

- Three drafts
  - EU Commission draft (Jan 2012)
  - EU Parliament draft (March 2014)
  - EU Council (probably June 2015
- Then discussions to reach consensus: Trilogue; i.e., three entities must agree on the final draft
  - European Commission
  - European Parliament (MPs representing the people)
  - European Council of Ministers (Ministers representing State Governments)

Territorial Application

- Regulation would apply to
  - processing of personal data in the context of activities of an establishment of a processor or controller whether the processing takes place in the European Union or not
  - companies that are established in third countries when:
    - offer goods or services to individuals located in the EU
    - monitor behavior of individuals located in the EU
- Regulation would NOT apply to
  - natural person without gainful interest, in the course of own exclusively personal or household activity
  - activities outside scope of EU law, e.g., national security, prevention, investigation, detection of crimes

Increased Power for DPAs

- Strengthen the independence and powers of the Data Protection Authorities:
  - –better equipped to handle complaints
  - –power to carry out investigations
  - –power to take binding decisions
  - –power to impose effective sanctions
- Provide means for more coordination between the DPAs so that there is more consistency in enforcement

New Rules for Consent

- Initial Rule:
  - When consent is required, it must be "specific, informed and explicit" and freely given
  - Individual must be aware that he is giving consent
  - Requirement for consent must be presented separately from other matters
  - Data subject must be able to withdraw consent at any time
  - Consent would not be legal basis for the processing if there is a significant imbalance between position of the controller and that of the individual
  - For child under 13, consent to be given by parent
  - Companies would have to be able to prove that the data subject has consented to the collection and use of the data

- Now: rules for consent likely to be narrowed

Streamlined Formalities

Significant savings resulting from streamlined formalities for cross border transfers

- No more notification
  - But, requirement for prior checking would remain for special kind of processing
- Interaction with one single DPA (currently being re-evaluated)
- Ability to use Binding Corp Rules in the 28 States

But … More Obligations

- Companies would have extended obligations with respect to data processing, including:
  - –establish detailed policies and procedures
  - –implement security measures
  - –disclose security breaches
  - –perform data protection impact assessment in special circumstances
  - –implement verification / audit mechanisms
  - –document compliance with Regulation

Emphasis on Security

- Increased emphasis on using appropriate security measures
- Security breach reporting for all companies
  - Definition of security breach much broader than in the US
  - Obligation to notify the DPA without undue delay
  - Obligation to notify individuals "without undue delay" if their data were adversely affected by the breach

Transfers Out of EU/EEA

- Binding Corporate Rules would be recognized as a valid instrument in all 28 Member States
- Procedures for BCR would be streamlined and extended so that BCR can be used by:
  - –data processors
  - –groups of companies
- Administrative cycles and obstacles would be eliminated

Complaints & Enforcement

- Individuals would have the right to
  - –Lodge a complaint with a DPA
  - –Seek judicial remedy against data controller or data processor
- Organizations and associations would have the right to lodge complaints and to seek judicial remedies on behalf of injured individuals if so requested by one or more data subjects

Significant Penalties

Warning in writing	*First, non-intentional non-compliance*
Regular periodic data protection audits	
Up to **100 Million** Euros or up to **5%** of annual worldwide G.I., whichever it higher	*Serious violations, e.g., processing data without legal basis, without complying with consent requirement; failure to adopt required policies* *If the controller or the processor has a valid European Data Protection Seal, fine of up to $100 million Euros or 5% annual GI ONLY in cases of intentional or negligent incompliance*

Questions?

Francoise Gilbert

Managing Director

IT Law Group

+1-650-804-1235

Email: fgilbert@itlawgroup.com

Blog: www.francoisegilbert.com

Book: www.globalprivacybook.com

IT Law Group