# IAPP PRIVACY ACADEMY 2012

October 10-12
San Jose, CA

## How the Proposed EU Data Protection Regulation Is Creating a Ripple Effect Worldwide

11 October 2012

Judy Schmitt
United Technologies Corp.
and
Florian Stahl
msg systems ag

www.privacyassociation.org/academy

# Agenda

- **Overview**
- Proposed changes
- **Ripple effects**
- Extra information

# Overview

# EU data protection background

- Goal: protect individuals against abuse of personal data
- Personal data protection is a fundamental right in the EU
  - Article 8 of the EU's Charter of Fundamental Rights
  - Article 16 (1) of the Treaty on the Functioning of the European Union (the Lisbon Treaty)
- 1995 – EU Data Protection Directive (DPD)
  - National legislation required to implement Directive
  - Rules across 27 Member States differ widely
- 2012 – EU General Data Protection Regulation (GDPR)
  - Proposal for a single European law
  - Commission staff administers and interprets the law
  - Local impact may not be understood yet
  - Ends "legal fragmentation and reduces administrative obligations (e.g. notification requirements)"

# EU Personal Data

"Personal data is any information relating to an individual, whether it relates to his or her **private, professional or public life**. It can be anything from a **name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address**. The EU Charter of Fundamental Rights says that everyone has the right to personal data protection in all aspects of life: **at home, at work, whilst shopping, when receiving medical treatment, at a police station or on the Internet**."

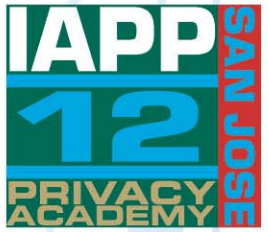
*From the European Commission's press release announcing the proposed comprehensive reform of data protection rules, 25 January 2012, Brussels, Belgium*

# General Data Protection Regulation

- Key changes* proposed in GDPR
  - Single set of rules
  - Responsibility and Accountability
    - Expand requirement to appoint Data Protection Officers
  - Data breaches (Breach notification)
  - Single DPA
  - Consent
  - Data portability
  - “Right to be forgotten”
  - Scope
  - Fines

** As per EU Commission’s press release 25 January 2012*

# Proposed Changes



# Single set of rules

- Valid across EU Member States
  - DPA Notification is no longer required
  - Prior authorization no longer necessary to transfer data if using BCR or Standard Contractual Clauses (SCC)
  - “Explicit criteria” established at the European level for the proposed “adequacy decisions”
- Single enforcement mechanism
  - Delegated and implementing acts (Article 86)
- Consumers and businesses interact with just one data protection authority
- Rules for applying EU standards to data controllers outside the EU
  - One set of rules for gaining approval for Binding Corporate Rules (BCR)

# Responsibility and accountability

- Data controller's responsibilities (Article 22)
  - Provide "documentation" (Article 28) instead of "notification"
  - Ensure data are secure (Article 30)
  - Perform data protection impact assessments (Article 33)
    - Consult and/or seek prior authorization from DPA if impact assessment seems risky
  - Appoint Data Protection Officers (Articles 35-37)
  - Verify / audit effectiveness of processing security

- Data processor's responsibilities (Article 26)
  - Act only on instructions of data controller

- Joint data controller's responsibilities (Article 24)
  - Determine who is responsible for what in relation to the data subject

# Responsibility – notice and access

- Notice (Article 14)
  - Notice requirements remain – and expanded
  - Must include retention time for personal data
  - Provide contact information for data controller, DPO(s), controller's representative, and relevant DPA

- Access (Article 15)
  - Individual may ask – at any time – if personal data are being processed
  - If so, data controller must provide specific information
    - Notice information, plus source of data and related consequences, if used for profiling (see Article 20)
  - Commission may require standard forms and procedures for verifying a person's identity (see Article 87)

# Accountability – design and impact

- Data protection by design and by default (Article 23)
  - Ensure GDPR regulations are designed into the development of business processes for products and services
  - Set privacy settings at a high level as a default
  - Collect only personal data necessary
  - Delete data as soon as possible

- Data protection impact assessment (Article 33)
  - Conducted when specific risks occur to the rights and freedoms of data subjects (Article 33.2)
  - Describe, assess and provide measures taken to mitigate risk
  - Seek DPA prior approval if impact assessment shows high risk

# Data Protection Officers

- DPOs are to ensure data protection compliance within organization (Articles 35, 36)
  - Must be appointed for all public authorities and for enterprises with 250+ employees
  - Two-year terms, with reappointment possible, but protected from dismissal during term
  - Either employee or service contractor
  - Must have expert knowledge of data protection law and practice

- Tasks (Article 37)
  - Advise of EU obligations
  - Ensure documentation is maintained
  - Monitor data breaches and associated communications
  - Monitor data protection impact assessments
  - Cooperate with country DPAs

# Data breaches

- Breach notification to DPA (Article 31)
  - Data controller to notify DPA "without undue delay and, where feasible, not later than 24 hours after having become aware" of the data breach
  - Extra information required if report is not within 24 hours
  - DPA requires:
    - Description of breach, including categories and numbers of data subjects and data records
    - Contact information
    - Recommended measure to mitigate breach
    - Consequences of personal data breach
    - Measures proposed to address the breach

- Breach notification to individuals (Article 32)
  - Required if adverse impact is determined
  - DPA may approve no notification

# Single DPA

- Supra-national data protection regulation
- Member State DPA authority (Articles 46 – 54)
  - EU Commission defines DPAs' authority, powers and duties
  - Independent, yet cooperate for administrative consistency
- Pan-EU cooperation (Articles 55 – 63)
- European Data Protection Board (Articles 64 – 72)
- Remedies, liability and sanctions (Articles 73 – 79)
- Specific data processing situations (Articles 80 – 85)
  - Freedom of speech
  - Health
  - Employment context
  - Historical, statistical and scientific research
  - Obligations of secrecy
  - Churches and religious associations

# Consent

- Valid consent must be explicit for data collected and purposes data used (Article 7; defined in Article 4)
  - Consent for children under 13 must be given by child's parent or custodian, and should be verifiable (Article 8)
- Data controller must be able to prove "consent" (opt-in)
- Consent may be withdrawn
- Consent cannot be used "where there is a significant imbalance between the position of the data subject and the controller" (e.g. employment situations)

# Data portability

- Right to data portability (Article 18)
  - Able to request copy of personal data being processed in a format usable by the person
  - Able to transmit electronically to another processing system, if data were processed based on consent or a contract

- Aimed at digital vaults
  - “Easy access to one’s own data”
  - “Freedom to transfer personal data from one service provider [such as social networks and photo-sharing websites] to another”

# “Right to be forgotten”

- Erasure of personal data (Article 17)
  - When individual withdraws consent
  - When an individual objects to processing personal data
  - When data are no longer necessary and “there is no legitimate reason for a company to keep” the data
    - Especially data collected when a person is under 18

- Focus of “right to be forgotten” has been on social media sites and on search engines
  - Person will “receive clear and understandable information when your personal data is processed.”
  - “Whenever your consent is required, it will have to be given explicitly before a company could process your personal data.”

# Scope

- Territorial scope (Article 3)
  - Controller or processor in the EU
  - Data subjects residing in the EU, if the processing
    - Offers goods or services to data subjects in the EU
    - Monitor behavior of data subjects in the EU
  - Controller not in the EU, but in a place where it applies by virtue of public international law.

- Representatives of controllers not in the EU (Article 25)

# Fines

- Administrative sanctions (Article 79)
  - "the supervisory authority *shall* impose a fine"
- Graduated fines
  - Warning
    - Non-intentional and by a person with no commercial interest or if the small organization (fewer than 250 employees) and processing is ancillary to the business
  - Up to €250K or up to .5% of annual global sales
    - Intentionally or negligently respond to requests by the data subject or the DPA
  - Up to €500K or up to 1% of annual global sales
    - Intentionally or negligently does not comply with GDPR
  - Up to €1,000K or up to 2% of annual global sales
    - Intentionally or negligently does not comply with specific GDPR regulations

# Next steps

- Commission provided proposal to the European Parliament and EU member States (meeting in the Council of Ministers) for discussion.
- Regulation is likely to be approved not until 2014
- Regulation will be enforceable in all Member States two years after it has been adopted (therefore, 2016?)
- Member States will also have a period of two years to transpose the provisions in the Directive into National Law.

# Ripple Effects

# Ripple effects … or tsunami?

*From EU Commission's GDPR press release and fact sheets:*

- "EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens."
- "By promoting global standards, the Commission's proposals will ensure continued European leadership in protecting data flows around the world."
- "Whenever controller's activities are related to the offering of goods or services to EU individuals, or to the monitoring of their behaviour, EU rules will apply."
- "EU rules will apply to companies not established in the EU, if they offer goods or services in the EU or monitor the online behaviour of citizens."
- "The globalised nature of data flows calls for a strengthening of the individual's data-protection rights internationally."

# Tsunami effect of GDPR

- "As privacy laws are internationally trending toward the EU model, U.S. businesses need to assess the way they do e-commerce abroad because compliance with foreign data protection rules and regulations may require them to change their business practices."

  – Cynthia Larose, Mintz Levin

- "The Cyber Intelligence Sharing and Protection Act Security (CISPA) might conflict with European [...] data protection law."

# How is data protection increased?

- Balanced approach in reforming current DPD?
  - Remains heavily bureaucratic
  - Reduces some and adds other administrative activities for businesses
- Gives more power to individual
  - Review of information held
  - Limit how information is used
- Strengthens enforcement
  - EU and national data commissioners can levy fines
  - DPOs in local organizations with more than 250 employees
- Global effect
- But: Decrease of protection level for some?
  - Strict implementation of current regulation in national law in some EU countries
  - Example: German law requires DPO > 9 employees

# Impact to data subjects / users

- European data subjects / users
  - Increases the level of data protection in general
  - Includes non-European based data processors offering their goods or services like social networks or web shops
  - Consistent approach for all organizations collecting and processing their data is easier to overview
  - Communication with the DPA where the data processor resides within Europe might be a burden (language?)
- Non-European data subjects / users
  - Increases the level of data protection if the data processor or controller is based in the EU
  - Non-European companies might adopt EU rules and offer them for non-European customers as well which would result in improved data protection in most of the cases

# Impact to employers

- Processing in the Employment Context (Article 82)
  - Individual EU Member States may still impose individual rules
- Regulation not specifically directed to employee personal data
- Life cycle of collecting and managing employee data:
  - Recruiting
  - Training and development, including career progression
  - Benefits administration
  - Payroll services, including compensation and rewards
- Business activities
  - Safety and workers health
  - Audit information
  - Communication, including email and directory of worker contacts
  - Contracts
- DPO appointments
- Labour regulations require consultation and/or consent from Works Councils – see Article 9.2(b)

# Impact to vendors / suppliers

- EU rules have to be adopted
  - When goods or services are offered to EU citizens, or
  - When their personal data is processed or stored
  - Increased effort for the implementation
- Knowledge about GDPR
  - People skilled with European Data Protection Regulation required
  - Increased cost
- Communication with DPA has to be set up
- Liability towards European DPA
  - Fines
  - Loss of reputation and customers
- Most global companies will be affected
  - Social networks (different configuration for Europeans?)
  - Web shops like Amazon
  - Internet services like Google
  - “Traditional” industries as well

# Proposals

- How to optimize efficiency of European Data Protection?

- **Proposal #1:** Establish a central European DPA
  - Improves standardization and coordination in practice
  - Single Point of Contact for Data subjects / users and non-European companies processing such data

- **Proposal #2:** Employment-related data should be governed by Regulations that differ from those governing customer/client data or social media data.
  - Relationship between employer and employee is unique
  - Requirement for data minimization should be enough
  - Do not include unstructured and auto-processed data (such as emails)

# Summary

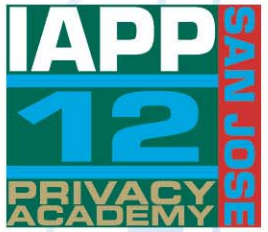
What is most important to consider as a privacy pro now?

1. Proposed changes to the **European Data Protection Regulation will affect you if** you have
   - European customers, or
   - European employees, partners, offices, etc.

2. Take your time to go through the changes of the GDPR and **identify new requirements**

3. Determine **what risks** to privacy **need real protection** considering your
   - Business situation (like reputation, customer satisfaction)
   - Legal requirements (future and current)

# Extra Information



# EU Commission Fact Sheets

Why do we need an EU data protection reform? (http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf)

How does the data protection reform strength citizens' rights? (http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf)

How will the data protection reform affect social networks? (http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf)

How will the EU's data protection reform strengthen the internal market? (http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf)

How will the EU's data protection reform make international cooperation easier? (http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_en.pdf)

How will the EU's data protection reform simplify the existing rules? (http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/6_en.pdf)

How will the EU's data protection reform benefit European businesses? (http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_en.pdf)

How will the EU's reform adapt data protection rules to new technological developments? (http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf)

# Comments to amend GDPR

BEERG

August 8th 2012

**Submission on Proposed EU General Data Protection Regulation (2012/0011) to the House of Commons' Justice Select Committee**

Executive Summary

- Business needs certainty and practicality from the legislation under which it operates. There are many varied and different personal data processing regimes across the EU.
- Such complexity already places the EU at a competitive disadvantage in attracting employers and encouraging job growth and economic development
- BEERG welcomes the idea of a Regulation – one set of clear and precise data protection laws to cover all EU and EEA members.
- Employee personal data is a special and distinct category of personal data. Processes and procedures that are appropriate for customer or client data are inappropriate for employee data. Multinational companies need to be able to manage multinational workforces and to be easily able to access personnel data to do this.
- We believe the proposed General Data Protection Regulation (GDPR) (2012/0011), as presented:
  - Fails to recognise the unique nature of personal employment data, and
  - Fails to strike a balance between the need to provide reasonable protection for the personal data of the individual with the unavoidable needs of business to be able to operate in an effective manner.

Specifically:

- Article 82 of the GDPR completely undermines the concept of a Regulation by allowing Member States to adopt rules additional to those already spelt out in the Regulation as regards employees' personal data.
- The Article 7 consent of employees provisions are overly restrictive., The consent of employees, or prospective employees, for such personal data processing as is essential to the employment relationship should be taken as a given.
- Requiring the appointment of data protection officers in all organisations with more than 250 employees is both unnecessary micromanagement and a major additional cost that would place the EU at an even greater competitive disadvantage.
- The Communication of Personal Breach requirements in the employment context are excessive and the proposed penalties proposed under the Regulation are too harsh without any element of proportionality.
- We are deeply concerned by the very broad powers the Regulation gives the Commission to adopt secondary acts without full, transparent democratic oversight or consultation with the social partners.

Introduction

1. The Brussels European Employee Relations Group (BEERG) provides a forum for European employee relations specialists and in-company employment lawyers to discuss issues of mutual concern. We have over 60 major transnational corporations in membership. We work closely with the Washington DC-based HR Policy Association. Together we work with over 300 major multinational corporations employing over 25 million workers globally.

2. Business needs certainty and practicality in the legislation under which it operates. At present, there are different regimes applying to personal data processing in different European Union Member States, with differences in the rules and their policing. This is problematic and threatens to become more so as several countries revise their approach to data protection to deal with the major developments in technology and behaviour since the original Data Protection Directive.

3. Accordingly, we welcome the idea of a Regulation – one set of clear and precise data protection laws to cover all EU and EEA members.

4. The European Union is rightly concerned that personal data exported outside the jurisdiction might be misused and therefore insists on safeguards before allowing its export. However, the discussion and attention around the proposed Regulation appears to have overly centred on issues relating to social media business and not the vast number of other types of business.

5. Our concern is with the rules regarding the personal data which business is obligated to hold and process in order to employ an EU workforce. Common to all businesses, and which needs to be discussed and addressed separately within the Regulation, is the need they all have to process employee personal data. Many also transfer such data from the EU to third countries. This is increasingly the case as more and more businesses make use of the enhanced processing capacity that "cloud computing" offers.

6. Employee personal data is a special and distinct category of personal data. The proposed regulation should recognize that basic employment data must be collected and utilized, and relieve employers from the same prerequisites and restrictions imposed for collecting and using consumer data, as long as employers follow a basic set of rules. It is inequitable and impracticable to lump together the concerns relating to data privacy and new social media with the data processing that every business must do on the employment relationship: hiring people, managing them and dealing with their departure.

Article 82

7. In the area of most concern to us, employment related personal data, Article 82 completely undermines the concept of a Regulation by allowing Member States to adopt rules additional to those already spelt out in the Regulation as regards employees' personal data. For multinational enterprises operating across Europe this may mean having to eventually comply with the Regulation and 27 different sets of domestic employment related data protection laws. Such complexity already places the EU at a competitive disadvantage in attracting employers and encouraging job growth and economic development against those world areas without such difficult and complex laws. We believe that Article 82 should be dropped completely and replaced by a specific chapter on the processing of employment-related personal data.

Article 7

8. The "consent" requirements (Art. 7) for employment related personal data in the Regulation are overly restrictive. There is, or should be, an understanding in the Regulation that the gathering, processing, and retention of relevant employee personal data by the employer is an essential part of an employment relationship, and should permit employers to do so as long as such data is used responsibly and that reasonable remedies exist should that trust be broken.

9. We believe that the consent of employees, or prospective employees, for such personal data processing as is essential to the employment relationship should be taken as a given.

employees with general notices to all EU employees en masse using whatever means is reasonable and on practicable timescales. Setting timescales of 24 hours for Notifications to Supervisory Authorities is not practicable, and overhasty Notification runs the risk of further error or misleading messages.

Mr Tom Hayes,
Executive Director,
Brussels European Employee Relations Group
tom.hayes@beerg.com

# Personal data processing

Principles (Article 5 in GDPR):

- Lawful, fair, and transparent manner to data subject
- Specific, explicit and legitimate purposes (and limited to those purposes)
- Adequate, relevant and limited to minimum necessary for processing purposes
- Accurate and up-to-date
- Kept no longer than necessary in a form which permits identification
- Under the responsibility and liability of data controller

# Personal data processing

Lawfulness of processing (Article 6 in GDPR):

- Consent by data subject (exception, see Article 7.4)
- Performance under a the contract
- Compliance with [other] legal obligations,
- Protect person's vital interests,
- Necessary in the public interest or with official authority
- Legitimate interest by data controller without overriding the data subject's rights

# Documentation

Documentation (Article 28 in GDPR)

- Name/contact details of the controller, representative, and/or Data Protection Officer
- Purpose and legitimate interest for processing
- Categories of data subjects and personal data
- Categories of recipients of personal data
- Transfers to third countries and the safeguards for sending data to organizations in third countries
- Retention time for categories of data
- Verification mechanisms to ensure protection of data

Maintained for all processing operations

*Note: This requirement replaces country-by-country registration under the EU Data Protection Directive.*

# Contact Information

**Judy P. Schmitt**
International Trade Compliance Program Office – HR
United Technologies Corporation
judy.schmitt@utc.com
860-731-9060

**Florian Stahl**
Senior IT Security & Privacy Consultant
msg systems ag
Florian.Stahl@msg-systems.com
+49 89 96101 1134