McKenna Long & Aldridge LLP

The EU Draft Data Protection Reform Package -its Significant Effects on Global Industry

Expected to apply as of 2016 (2 years after entry into force)

OUTLINE

- I. Introduction – Legislative Process
- II. Objectives
- III. Basic Principles
- IV. Main Points
- V. The Current and New Rules on Transfer of Data from the EU to the Third Countries
- VI. The Current Rules for Exchange of Data between EU and US: The Safe Harbor Principles
- VII. Data Protection in the US: White House Paper
- VIII. US Consumer Privacy Bill of Rights
- IX. Enforceable Codes of Conduct
- X. Police and Criminal Justice Data Protection Directive
- XI. Summary

I. INTRODUCTION - LEGISLATIVE PROCESS

European Commission (EC) **Draft Data Protection Reform Package:**

- Proposal for Data Protection Regulation (DPR).
- Delegated and Implementing Acts of the EC (+/- 27)
- Proposal for Police and Criminal Justice Data Protection Directive.

Current status:

- Publication of the Proposals on January 25, 2012
- 'Subsidiary principle' concern of Germany and Austria
- The Proposals will now pass to the European Parliament
- The EU Member States meeting in the Council for discussion.

II. OBJECTIVES

- New challenges since Data Protection Directive 95/46/EC ('Directive 95/46 EC')
- Digital society
- Innovative uses of new technologies
- Building consumer trust
- Protecting personal data
- Creating jobs and future wealth
- Interoperable policy framework for Cloud computing and the Internet of Things ('IoT')

III. BASIC PRINCIPLES

- Uniform and coherent data protection rules applicable in all EU Member States.
- “One-stop-shop” principle: one national data protection authority (Lead Authority') in the Member State of “main establishment”.
- Stricter rules and procedures for both EU and non-EU companies.
- More rights /transparency/protection for the data subject.

IV. MAIN POINTS

1. Scope
2. Key definitions: “Controller” and “Processor”
3. New Obligations for all Controllers
4. Obligations for non-EU controllers
5. Concept of an explicit consent
6. E-commerce: location data and online identifiers
7. Obligation to notify personal data breaches
8. New obligations for processors, impacting Cloud Computing
9. New obligations for processors, impacting the IoT
10. Remedies/Significant sanctions

IV.1. Scope

- The processing of personal data wholly or partly by automated means, and the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system, in the **context of the activities of an establishment of a controller or a processor in the EU**.

- It will impact on **Controllers and Processor**.
- It will affect both **EU and non-EU** companies.

- Definition of **“an offer of goods and services**” and **"monitoring of data subject behavior"** for non-EU controllers.

IV.2. Key Definitions: "Controller" and "Processor"

- Definitions

  "**Controller**" : a natural or legal person, who alone or jointly determines the purposes, conditions and means of the processing of personal data. (same as in the current Directive 95/46)

  "**Processor**" : a natural or legal person who processes personal data on behalf of the controller. (same as in the current Directive 95/46)

  "Joint Controller" : a controller who determines the purposes, conditions and means of the processing of personal data jointly with others; a processor who processes personal data other than as instructed by the controller.

- Non adaptation to the reality of the on-line and digital market.
- Examples: Cloud computing, Internet of Things, Electronic Payment Systems, E-Invoicing, Facebook (complaint of 18th September 2011 against Facebook Ireland Ltd), SWIFT case.

IV.3. New Obligations for all Controllers

- The Controller **and the Processor** shall demonstrate that data processing is in compliance with the Regulation by:
  - a) keeping documentation of all processing operations, description of mechanism.
  - b) implementing data security requirements, adopting policies.
  - c) sectorial codes of conduct.
  - d) performing a data protection impact where process operations pose risks to the rights of data subjects.
  - e) acquiring prior authorization or prior consultation of the supervisory authority where needed.
  - f) designating a data protection officer.
  - g) cooperating with the supervisory authority.

  Emphasis on compliances → impact on business operations.

IV.3. New Obligations for all Controllers

- In addition, Controllers have to:

  a) implement appropriate technical measures throughout the whole processing procedure to ensure the protection of the rights of the data subject (privacy by design principle)

  b) implement mechanisms ensuring that, by default, only those personal data are processed which are necessary for each specific purpose (privacy by default principle)

IV.3. New Obligations for all Controllers

- Vis-à-vis the data subject:

  a) providing access on the data process - making request for information available in electronic form to the data subject.

  b) profiling will be regulated.

  c) the right to be forgotten and erasure.

  d) the portability of data.

  e) informing the data subjects about the storage period of their data.

IV.4. Obligations of non-EU controllers/processors: Representatives under Directive 95/46/EC

- Controller not established on EU territory and making use of equipment, automated or otherwise on the territory of a Member State, unless the equipment was used only for purposes of transit through the territory of the EU. Example : e-invoicing and electronic payment systems.
- Appointment of a representative in the EU.
- Notification of intention to process data to data protection authorities in the EU Member States concerned.
- Non-EU processors were falling outside the scope of national legislation.

IV.4. Obligations of non-EU controllers: Representatives under the new regime

- Any controller not established in the EU whose **'processing activities relate to the offering of goods or services to EU subjects'** or **'who monitors their behavior'** shall have the same obligations as EU controllers ? Direct or indirect ?

  Example: US companies marketing their products in the EU through websites or running social networks.
- Must designate a representative in the EU, who can be addressed by all competent authorities.
- No specific rules for processors.

IV.4. Obligations of non-EU controllers: Representatives under the new regime

- **Exceptions:**
  a) established in a third country where the EC has decided that the third country ensures an adequate level of protection.
  b) employing fewer than 250 persons ('SME').
  c) public authority or body.
  d) offering only 'occasionally' goods or services to data subjects in the EU.

IV.4. Obligations of non-EU controllers: Representatives under the new regime

- **What are the main concerns?**
  - a) Extensive liability of representatives (can be addressed by any competent authority in any Member State) !
  - b) Enforcement of rules against companies with no representative ?
  - c) What about processors for example based in third countries and not obliged to have a representative and their liability ?
  - d) Compliance of the "representative requirement" with the free trade principles of GATT ?
  - e) Considerable cost of compliance / operational business impact ?
  - f) Users forced to make decisions about privacy well before using a particular service !

IV.5. Concept of an explicit consent

- **Consent**

  "specific, informed and explicit indication of wishes either by a statement or by a clear affirmative action by which the data subject signifies agreement to personal data relating to them being processed".
- Removal of the distinction between "personal" and "sensitive" data of Directive 95/46.
- Burden of proof lies on the industry.

IV.5. Concept of an explicit consent

- Explicit consent for the collection of “anonymous” data.

- Valid consent of a child (i.e. a person below 13 years) when given by the child's parent or custodian.

IV.6. E-commerce: location data and online identifiers

- A person can be identifiable solely on the basis of location data and online identifiers.

- Any IP address to be treated as personal data.

- What about “Cookies”? Profiling ? Should there be an explicit consent every time a subject re-visits the webpage? For example: preferred choices when visiting websites. Should companies “reconstruct” their web pages so that consent is given by the user in advance of entering the page?

- Example: Targeted advertising by a newspaper’s website that can track the user’s location through his IP address and adapt the projected advertisements accordingly.

IV.7. Obligation to notify personal data breaches

- **Controllers** must notify the Member State data protection authority (and also the data subject if he is adversely affected) of any personal data breaches.
- **Time limits for notification**: Without delay; where possible, not later than 24 hours after the breach. Is this realistic if different parties involved ?
- **Processors**: alert and inform the controller immediately after the breach.
- **Breach:** Claims for damage, administrative sanctions, etc.

IV.8. New obligations for processors, impacting Cloud Computing

- **DPR territorial scope: How about cloud computing industry** ? ("providing of services over the Internet which are connected with storage of data in the cloud").
- Legal Issues :
  a) "Means" of the processing defined by both customer and the hosting provider.
  b) Reduction of the level of control.
  c) Are sub-processors regulated?
  d) Contractual limitation of liability by the hosting providers.
  e) Difficulty to "locate" the data because the place of operation of the servers is often unknown.

IV.8. New obligations for processors, impacting Cloud Computing

- **Obligations of processors under the new framework** (including sub-processors in cloud computing?) :
  - a) carry out data protection impact assessment.
  - b) obtain prior authorization and consultation of processing.
  - c) designate a data protection officer for enterprises employing more than 250 persons.
  - d) provide any necessary documentation.

- **Potential impact on cloud computing industry?** Risk related to the loss of the competitiveness of the EU industry in this area.

IV.9. New obligations for processors, impacting the Internet of Things (IoT)

- IoT: Seen as a subset of the cloud. Things, including everyday objects, which are readable, recognizable, locatable, addressable and/or controllable via the Internet based on sensor based technology.
- Focus needs to be on protecting privacy and enabling innovation in the context of the societal benefits of IoT apps like the smart grid, sustainable consumption, and smart logistics.
- Communications:

  a) Machine-to-machine

  b) Machine-to-person

Concerns: Unauthorized processing of personal data by objects acting as controllers.

IV.9. New obligations for processors, impacting the Internet of Things (IoT)

EC's initiatives on the IoT:

- EU Formal Expert Group on the IoT through 2012.
- A public consultation will begin in the next few weeks.
- Goal must be a horizontal interoperable privacy framework for the IoT and the Cloud and the EU must avoid additional privacy regulation over and above the proposed EU data regulation for the IoT and the Cloud.
- Being attached to technology neutrality and principle-based legislation, the objective of the current data protection reform should be to develop an overarching, horizontal, consistent and clear privacy framework that should be shared across borders and across sectors.

IV.9. New obligations for processors, impacting the Internet of Things (IoT)

- **Does the proposal tackle issues related to the IoT?**

  No reference to the IoT

  Definition of controller and processor cannot be broadened to cover objects communicating via the internet.

IV.10. Remedies/Significant sanctions

- Remedies of data subjects:

  a) Judicial remedy against **controller or processor**

  b) Judicial remedy against supervisory authority in EU

  c) Administrative remedy by lodging a complaint before the competent authority

  d) Right to claim compensation from controller or processor for any damage suffered.

.

IV.10. Remedies/Significant sanctions

- Risks for companies : Substantial fines for breaches.
- **Example:**

  Fines up to 1 000 000 EUR /company: up to 2 % of its annual worldwide turnover for:

  a) non adoption of data protection policies or non implementation of appropriate measures.

  b) processing of personal data without prior authorization or prior consultation of the supervisory authority.

  c) non designation of a representative.

  d) not alerting or notifying in timely manner of a personal data breach.

V. The Current and New Rules on Transfer of Data from the EU to the Third Countries

The Current system

•Transferred only from the countries in the EEA to countries which provide adequate privacy protection.
•Exceptions: disclosure of data outside the EEA with the unambiguous consent of the individual concerned or for the conclusion of a contract or legally required under the law of an EEA Member State (difficulty for example Whistle Blower System under Dodd Frank Act) or to protect the vital interest of the data subject.
•Tailor made corporate rules authorized by the national data protection authorities.
•Standard contractual clauses of the EC (EC Decisions C (2001) 1539 and C (2004) 5271))

The "Working party on the Protection of Individuals with regard to the processing of personal data", monitors the existing legislation in third countries on data protection.

V. The Current and New Rules on Transfer of Data from the EU to the Third Countries

Countries providing adequate protection as of 29 March 2012:

- Andorra
- Argentina
- Australia
- Canada
- Switzerland
- Faeroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey

V. The Current and New Rules on Transfer of Data from the EU to the Third Countries

According to the New Proposal, export of data from EU to non-EU controllers or processors only if:

- Specific EC decision that the third country or a specific processing sector within a third country ensures an adequate level of protection, *or if no such decision*
- One of the exceptions similar to these of the Directive 95/45 is in place.
- Adoption of "Binding corporate rules" by the controller or processor (one stop principle) *or*
- Use of Standard data protection clauses (one stop principle) *or*
- Authorized in advance by a Member State contractual clauses between controller/processor and recipient of the data.

VI. The Current Rules for Exchange of Data between EU and US: The Safe Harbor Principles

Current system of exchange of data between Europe and US, likely to be impacted by the new system.

- US not among the countries listed in the EU's list of third countries that ensure an adequate level of protection:
- **Safe Harbor**: agreement between the EU and the US enabling US companies to demonstrate their compliance with the Data Protection Directive 95/46/EC: US Companies obtain a certification of compliance with EU data protection principles.
- Obligation to inform individuals about collection and use of their data. Individuals must be able to opt out of the collection and forward transfer of the data to third parties.

VII. Data Protection in the US: White House Paper

- The Obama Administration in late February released its long-awaited report outlining a framework for U.S. data protection and privacy policy.
- The report, entitled, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Global Innovation in the Global Digital Economy" proposes a consumer privacy bill of rights based on the individual's right to exercise control over what personal data companies collect from the individual and how companies use the data.

VIII. US Consumer Privacy Bill of Rights

- **The US Consumer Privacy Bill of Rights** sets forth individual rights and obligations of companies in connection with personal data based on the fair information practice principles:
- Individual control
- Transparency
- Respect for Context
- Security
- Access and Accuracy
- Focused Collection
- Accountability

IX. Enforceable Codes of Conduct

- Developed through a broad multi stakeholder process between industry, privacy advocates, and consumer groups to develop enforceable codes of conduct to implement the Consumer Privacy Bill of Rights.

- FTC enforcement of these new voluntary codes using its authority to prohibit unfair or deceptive acts or practices.

- Increase global interoperability between the sectoral US data privacy framework and the EU through mutual recognition and enforcement cooperation.

X. Police and Criminal Justice Data Protection Directive

- **Aim:** to facilitate the free flow of personal data between EU police and judicial authorities.
- **Scope of the Directive:**

  Processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

  Processing of personal data by automated means, and the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
- **Exceptions:**

  Data processed in the course of activities falling outside EU law; data processed by EU institutions, bodies, offices and agencies.

X. Police and Criminal Justice Data Protection Directive

- **Main provisions:**
  - a) General prohibition of processing by competent authorities of special categories of personal data (revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, of genetic data or of data concerning health or sex life.)
  - b) Member States may adopt legislative measures restricting the right of controllers/processors of access to data in the areas of police and criminal justice.
  - c) Obligation of every controller to notify breaches to the supervisory authority within 24 hours; processor must also inform the controller about breaches.
  - d) Obligation of the competent authority acting as a controller or processor to appoint a mandatory data protection officer.

X. Police and Criminal Justice Data Protection Directive

- Effects to the industry?

  a) Obligation of Internet Service providers to cooperate with the designated national supervisory authorities.

  b) Obligation to alert users about use of their personal data in the course of an investigation by the competent authorities.

  c) Operational consequences for the business.

XI. SUMMARY

- **DPR significant impact for both EU and non-EU companies**, through:

  a) **"One-stop-shop" principle and lead DPA.**

  b) Introducing new obligations with focus on compliance.

  c) Balancing data privacy against competition – sanctions 2 % annual worldwide turnover.

- **The Industry should consider advocacy opportunities as still aspirational legislation.**

MORE INFO

- Ales Bartl, Associate, abartl@mckennalong.com
- Hendrik Bossaert, Associate, hbossaert@mckennalong.com
- Dan Caprio, Senior Strategic Advisor, dcaprio@mckennalong.com
- Orestis Omran, Contributor, TMLA@mckennalong.com
- Nora Wouters, Partner, nwouters@mckennalong.com