The status
of the future European data protection regime

Claire BERNIER

Thursday, 27 February 2014

ITECHLAW®
INTERNATIONAL TECHNOLOGY LAW ASSOCIATION

ALTANA
Société d'Avocats à la Cour de Paris

CHANGES IN EXISTING PROVISIONS

.

ABOLITION OF THE OBLIGATION OF NOTIFICATION

Past : importance of preliminary formalities = **Future** : abolition of the obligation of notification

- ✓ lighten significantly the administrative burden
- ✓ strengthen the powers of the supervisory authorities
- ✓ Increase the responsibility of the data controllers

➢ Global annual savings for companies : 2.3 billion Euros.

ONE-STOP SHOP (ARTICLE 51)

One-stop shop system within the EU: "*the competent authority should be the supervisory authority of the Member State in which the controller or processor has its main establishment where the processing of personal data takes place in more than one Member State*" (**section 2**), to ensure unity of application.

CRITICISMS

- **Legal uncertainties on the concept of "main establishment"** - defined as the place where "*the main decisions as to the purposes, conditions and means of the processing of personal data are taken"*
- **Risk of data dumping**: development of bypass strategies in selecting the place of establishment according to local constraints.
- **Competition between authorities** : national authorities of aggrieved citizen don't have jurisdiction and authorities may contest other authorities' decisions.
- Draft report by Jan Albrecht on the 17 December 2012 :
  - competence of the supervisory authorities should also be based on the citizen's place of residence;
  - a lead authority to investigate cross-border situations with a real cooperation between the supervisory authorities

DATA PROTECTION OFFICER (ARTICLES 35 TO 37)

- **compulsory appointment of a data protection officer** for two years minimum where:
  - the processing is carried out by a public authority or body or an enterprise employing 250 persons or more,

  OR
  - the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects

- a **group of undertakings** may appoint a single data protection officer (for enterprise over 250 employees).

- designation on the basis of **professional qualities and expert knowledge of data protection law** and practices

- The data protection officer may be an **employee of the controller or processors**, or fulfill his or her tasks on the basis of a **service contract**

NEW PROVISIONS

.

THE RIGHT TO BE FORGOTTEN (ARTICLE 17)

- **erasure of all personal data on simple request if the controller has no legitimate reason for keeping it**

- **resale right**: "*where the controller has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data*".

CRITICISMS

- Use of a non legal terminology ("child" to be understand as "*any person below the age of 18 years*"). Quid about legally incapacited adult ?)

- **Recent meaning of the terminology "right to be forgotten"**

- Iechnically incorrect as no erasure is possible (due to reduplication of the data – crushed instead of deleted). Quid about desindexation?

ACCOUNTABILITY (ARTICLES 22 TO 29)

- **Continuous and dynamic compliance process** with the Regulation owing to a set of binding rules and **<u>good practices</u>**. "*the controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed incompliance with this Regulation*":
  - ✓ keeping the documentation;
  - ✓ implementing the data security requirements;
  - ✓ performing a data protection impact assessment;
  - ✓ complying with the requirements for prior authorization or prior consultation of the supervisory authority;
  - ✓ designating a data protection officer.

- The controller shall implement **mechanisms to ensure the verification of the effectiveness** of the measures.

- "**Privacy by design**" (article 23): the controller shall implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

- "**Secure by design**" (article 30) : the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.

➡ Legal issues : accountability vs liability

RISK ASSESSMENT (ARTICLES 32 TO 35)

- **Preliminary impact assessment of processing data** on the protection of personal data where processing is likely, by the nature of the data collected or the purpose of processing, ***to affect adversely the rights and freedoms of data subjects*** (processed data concerning sex life, health, race, ethnic origin, etc., or processing aiming at assess work performance, solvency, the economic situation, the behavior, etc).

- The preliminary impact assessment must provide a ***general description of processing, an evaluation of the risks for the rights*** and freedoms of data subjects and the measures implemented to protect the data. The data subjects must be consulted for advice.

PENALTIES (ARTICLE 79)

- **Strengthening of penalties** (administrative sanctions) applicable to controllers by the national authorities. Depending on the violations :

  For a natural person : a fine up to **100 000 000 EUR**

  In case of a legal entity : a fine up to **5% of the annual worldwide turnover**

Contacts

Claire BERNIER
Co-founding partner
LD : 00 33 1 79 97 92 79
Fax : 00 33 1 79 97 97 69
cbernier@altanalaw.com

ALTANA
Société d'Avocats à la Cour de Paris