



## **About Security Breaches and other selected new legislative provisions.**

LSEC Conference – Leuven  
February 9, 2010

Professor Y. POULLET  
Universities of Namur and Lieger  
Directeur du CRID  
yves.poullet@fundp.ac.be  
<http://www.droit.fundp.ac.be/crid>

### **Part. I Security Breaches**



- A new concept, new obligations  
and new powers granted to DPA

## Introduction – table of contents



**e-Privacy Directive recently amended (Nov. 25, 2009) introduces provisions about security breaches..**

- **What does it mean**
- **Which consequences for which companies?**
- **Which new competences for DPA?**

3

## Security Breach: a new concept



- **Multiplication of cases: the UK cases about health and fiscal data, the VENDETTA Belgian case,...**
- **Problem of unlawful or accidental destruction, loss, alteration, unauthorized disclosure or access to personal data**
- **Risks of identity thefts, financial losses and reputational damages**
- **Caused by hacking, malfunctioning of IS, etc...**

4

## Security Breach: a new concept (2)



### 1. Originally, a US Concept

**At the States level: see the impressive list (48 States have adopted Security Breach notification Laws)**

**At the federal level: The « Data Accountability and Trust » still a bill presently in discussion at the Congress.**

**Sect. 3 (a) « Any person engaged in Interstate trade and who owns or possesses electronic personal data shall notify a breach to individuals, if the breach leads to an unauthorized third person acquiring the data, and also to the FTC. »**

5

## Security Breach: a new concept (3)



### 2. Main objectives (consumer privacy approach)

- **To prevent and minimize adverse effects for individuals – to give them an opportunity to take appropriate measures for limiting their damages**
- **To assert the accountability of the data controllers and processors towards data subjects**
- **To give the FTC an adequate information in order to take if needed or possible appropriate measures**

6

## Security Breach: a new concept (4)



### 3. The review of the e-Privacy Directive and the introduction of the concept

- **From the telecom package to the adoption (November 25th) of certain amendments to the Directive 2002/58 to be transposed before May 2011**
- **The introduction of the « EU Security framework » and the battle about its scope**
  - *The European Parliament, EDPS and Art. 29 WG position: enlargement of the obligation in cases of security breach to all IS services (on line banking services, Web 2.0 platforms, Cloud computing services, hosting services, etc.)*
  - *The opinion of the Commission and the Council of Ministers...and their victory: « in connection with the provision of publicly available electronic communication services » (art. 2b) = ISP, certain RFID systems, mobile and T.O. webmail services (?)*
  - *BUT « explicit mandatory notification scheme applicable to all sectors should be introduced at Community level as a matter of priority »*

7

## The EU Security Breach Framework – Systematic Analysis



### I. The background principles:

- Far beyond the Security Principle laid down in the DP directive
  - Art 17 of the Directive 95/46 and the obligation of data controllers (are T.O. data controllers?) to implement appropriate technical and security measures against any unlawful disclosure, loss or alteration, against any unauthorized disclosure or access and any other unlawful processing. »
  - The increased obligations imposed by the Amending Directive (art. 4.1 bis)
  - The obligation to notify the security breaches, a way to improve data security practices
- A first recognizance of the US and APEC « accountability principle » (see also, the Madrid 2009 global principles): the idea of linking processing of personal data and accountability for these processing towards individuals and authorities.

8

## The EU Security Breach Framework – Analysis (2)



### II. The Definition (art. 2 (h))

- Also in cases of accidental failures
- Data security breach covers cases where « personal data » are compromised - notion of data very broad including cookies and traffic data (see in US limitation to certain personal data) – personal data in all format possible and not only in electronic form (see the UK case)
- Not only in cases of confidentiality breaches but also in cases of integrity and availability breaches
- Even if the personal data are processed by an external data processor (Quid if you use a transmission chain involving both publicly available e-comm. services and not publicly ones?).

9

## The EU Security Breach Framework – Analysis (3)



### III. The obligation to notify (art. 4.3)

- Notification to **authorities** (DPA): all Data Security Breaches ... even if there is no « adverse effects » for data subjects - Need for selective policy ?
- Notification to **data subjects** (not necessarily the subscriber or the user?) only « *when the breach is likely to affect their personal data and privacy* »
  - *Examples (Recital 61) : identity theft or fraud, physical harm and significant reputational harm ( beyond economic loss)*
  - « likely » - *need to take into account the context more than a pure probability but... – to be estimated by the D.C but under the control of the DPA. - against the risk of over-notification?*

10

## The EU Security Breach Framework – Analysis (4)



### III. The obligation to notify (art. 4.3)

- Notification to data subjects ...
  - *Exceptions if technological protection measures have been taken and render the data unintelligible (not only make more difficult the access) + 2 conditions: 1. approval of the authority and 2. measures actually implemented*
  - *Timing of the notification: « without delay » in order to take the necessary precaution » for alleviating or even for avoiding any damages.*
  - *How to notify? Media not defined (through e-mail, via a web site, by newspaper? ) criterion of the appropriate mean in function of the recipients to be informed and the relationship between the DC and them.*

11

## The EU Security Breach Framework – Analysis (5)



### III. The obligation to notify (art. 4.3)

- Notification to data subjects ...
  - *Content: to be decided in function with the objective – it means not only the relevant incident but also the actions to be taken (through by instance a call centre) – need to have an effective notification (understand the risk and describe adequately the measures to be taken) – no confusion with advertisement or spams, etc. – possibility for DPA to draw up standard forms of notification.*

12

## The EU Security Breach Framework – Analysis (5)



### IV. Enforcement of the provisions

- by DPA
  - *Audit by DPA (art. 4.4) after a notification of a security breach or independently of any notification (preventive measures)*
  - *+ all investigative powers for monitoring the respect of the security principle and for sanctioning any infringements (article 15a beyond article 28 of the D.P. Directive)*
- by Jurisdictions : notification to DPA and to D.S does not mean exoneration of liability but in cases where effective mitigating measures were possible and advised reduced liability.

13

## The EU Security Breach Framework – Analysis (5)



### IV. Enforcement of the provisions

- Technical implementing measures through Comitology (art. 4.5): EU Commission after consultations of ENISA, Art. 29 WG and EDPS (art. 14 a)
  - *Examples:*
    - To define certain sensitive data which creates adverse effects (e.g. health data)
    - To impose the format for the notification and their content
    - To impose a delay for notifying...
    - To impose technical measures for protecting data

14

## PART II



- TOWARDS A REGULATION OF THE TERMINALS

### – The articles 5.3 and the article 14.3 of the e-privacy Directive

15

### About « terminals » : the two provisions



- **Art. 5.3:** «Member States shall ensure that the use of electronic communications networks to store **storing of** information, or to **gaining** access to information **already** stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned **has given his or her consent**, having been provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. »
- **Art. 14.3.** «Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications.

16

## Table of content



- Why that choice?
- The article 5.3 and its significance
- A few additional remarks
- The article 14.3 and its significance
- A few additional remarks

17

## From DP directive 95/46 to the amended e-Comm. Directive 02/58



- Directive 95/46 reduces data Protection to a dialog between D.C and D.S, by creating new duties for the first one and new rights to the second one.
- Between these two parties, modern IS are characterized by the crucial role played by interfaces like the infrastructure and the terminal
- These interfaces are not (or no more) regulated or under the control of public authorities.
- As regards terminals, they are more and more various (from laptop to RFID), ubiquitous (accompanying and revealing all events of our daily life) and functioning in an opaque way permitting to a lot of (third) parties to trace and/or profile the DS even if not directly or indirectly identifiable. + possibility to combine different terminals (e.g. Mobile and RFID).
- They create new risks of Privacy Threats

18

## The article 5.3



- SCOPE
  - Risks of intrusion into the terminals viewed as an electronic domicile
  - Through spyware, web bugs, hidden identifiers (notably cookies), possible reading at distance
  - Coming from the connection or from any connected materials (?)
- REGIME
  - Forbidden except if
    - *Legitimate purposes and proportionate content and duration (problem of consent)*
    - *Duty to inform (Recital 25)*
    - *Opt-in system*
  - Permitted if
    - *Necessary for providing the I. service required (e.g. screen simulator)*
    - *for the sole purpose of carrying out or facilitating the transmission of a communication*
    - *To check if there is no contra-indication with software already placed into the terminal.*

19

## Beyond the article 5.3.



- Terminal considered as a « virtual domicile » to be protected as a private home
  - Reminder : article 8 of the C. of E. Convention or article 7 of the EU Charter on human rights : increased protection of the intimate sphere beyond DP directive
  - Confirmation of this approach by the B.Verf. G hof by creating a new constitutional right (Feb. 27 2008) against online searches by LEA (Trojan horse): The «*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*» with only few exceptions in case of very serious crimes

20

## Beyond art. 5.3



- Application of the criminal provision about « Hacking » (See C.of E. Convention on Cybercrime, art.2 ): *«Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. »*

21

## Article 14. 3



- Regime
  - Possibility for the EU Commission to require adoption of mandatory standards in order to ensure that the terminal is construed in a way compatible with the right of users to protect and control the use of their personal data
  - ...if possible according to the principle of technological neutrality.
- Significance
  - Possibility (or duty) for the EU Commission to impose the implementation by default of PETS to terminal equipments' suppliers (see already, **the Commission Communication May, 2, 2007**) **promoting D.P by PETS: "PETs are a prerequisite for creating confidence in the I.S. "**
  - The right to a transparent and privacy compliant terminal

22

## Beyond article 14.3.



- A first partial application: the Article 29 W.P opinion on RFID (Jan. 19, 2005) and the EU Commission's Recommendation of May 2009.:
  - Principle drawn down from Recital 2 of the DP Directive : « *Data processing systems are designed to serve man: (...) they must ... respect their fundamental rights and freedoms, in particular the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of the individuals* ».
  - Consequences
    - *As regards manufacturers of RFID technology and standardization bodies : obligation to ensure that DP compliant technology is available through a Privacy Impact Assessment*
    - *It means furthermore :*
      - Information requirements
      - Right to tag content access, rectification and deletion.
      - Security related obligations (encryption techniques)
      - Duty to implement tag disablers

23

## Any conclusions



- Security breach, today a text... tomorrow a reality for each ISSP?
- Terminals and « privacy by design » - not an option, a duty. « The answer to the machine is in the machine » (Ch. Clarke about IPR violations).
- Extension of the Privacy Protection to Information Systems and Terminal Equipment Products providers.
- Reasons for a proactive attitude of EU: the environmental policy « precedent ». To bet on Privacy is really an economic investment at mid term.

24