



CBPL
Commissie voor de bescherming
van de persoonlijke levensfeer

CPVP
Commission de la
protection de la vie privée

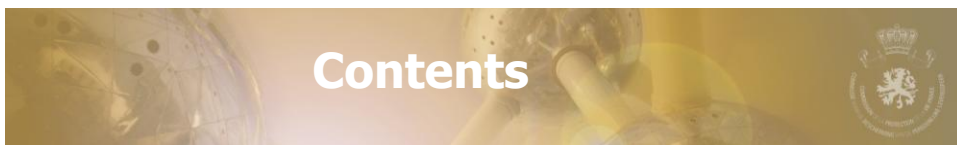
CPP
Commission for the
protection of the privacy

ASP
Russschuss für den
Schutz des Privatlebens


The need for a clear Data Breach Notification Law

Panel discussion

LSEC, Leuven



Contents



- DBN according to Belgian DPA
- Field of application
- Issues with DBN
- Conclusion ?

1. Official national opinions



Draft "wishlist" for Parliament : include general DBN obligation in article 16 DP Law.

One official Opinion 06/2009 of 18 March 2009 regarding project of law on the creation of a central car database

Context =

- e-gov application
- high risk of abuse due to broad local use of data by a.o. private sector (a.o. car sales reps) etc...
- several data breach incidents since 90's (DM for secure cars) due to confusion re legitimate use and soft law approach by industry

2. Application ?



- Directive 2002/22/EC : why sectoral approach with scope mainly on ISP and telecom operators ?
- Why not single & general approach that covers also
 - private networks
 - other sensitive / high risk operations
 Ex : online banking, online e-health platforms, private data warehouses,.... (EDPS Opinion 10 April 2008, OJ 18/07/2008, Opinion WP 29 nr. 150, 2/2008)
 - high risk e-gov applications

3. Issues



- First Priority = main legal & practical measures should be first in place to ensure adequate enforcement of compliance with DP law (i.e. rather focus on examples such as class action than DBN, good security practise decrease the need for DBN)
- "costs vs. benefits ratio" of DBN
 - additional cost for data controllers
 - limited analysis capacity with DPA's (also handling of Q&A's, complaints, prior checking in opinions/authorisations, awareness-raising...)
 - Risk of "over-notification" & backlog with DPA's
 - DBN should not be a formality but adapted to context & risk

Note : see experience with application of general obligation of notification in article 18 Directive 95/46/EC

3. Other issues



- DBN vs. existing professional secrecy obligations based on law / NDA's,...?
 - DBN is not a full solution for other issues
- general low level of DP & security compliance for processing via websites & private networks
 Hearing Parliament on ICT Security, 23/01/2008
 Lee & White Consultants, december 2005 (websites)
- problem of ID theft
 Problem is not to find a legal basis to prosecute ID theft
 Problem = dark number + need for simple procedures to register victims of ID theft in files such as consumer credit,...

4. Conclusion ?



SBN has potential / added value for some sectors as practical measure

BUT ... SBN is not a priority unless

- The main legal & practical measures are in place to guarantee adequate compliance with DP law (article 28 Directive 95/46/EC)
- SBN needs a clear legal basis in (a single) national (DP) law (article 22 Constitution)
- SBN is not the only measure, but is combined with other practical measures (example : class action, admin fines, procedure ID theft, ...)
- SBN is targeted , i.e. to areas with high risk or processing of sensitive data (e-commerce, e-gov, financial data, high risk technologies,...) that induce a manageable n° of notification to DPA's

CBPL
 Commissie voor de bescherming
 van de persoonlijke levenssfeer

CPVP
 Commission de la
 protection de la vie privée

CPP
 Commission for the
 protection of the privacy

ASP
 Ausschuss für den
 Schutz des Privatlebens

Thank you for your
 attention

Dieter VERHAEGHE
 Legal Counsel