

From a notification-based to a multi-faceted model of supervision

How to deal with change?

Lessons learnt after 3 years developing CNIL's fully-fledged enforcement policy

London initiative – Enforcement Workshop – Brussels, 24 April 2007

From 6 January 1978 to 6 August 2004

CNIL's model of supervision mostly relied on prior notification and prior checking:

- Prior notification (private sector)
- Prior opinions (public sector)

Enforcement powers were scarcely used:

- ~15 inspections per year since 1978 (127 in 2006)
- Only 54 warnings issued and 34 cases referred to the Public Prosecutor in 25 years (1978-2003)

Internal organisation and staff culture matched this policy accordingly

Since August 6, 2004 : the new DPAct

The law requires a balance between *ex ante* and *ex post* checks

- Availability of new tools for simplification of *ex ante* checks (DPOs, fast-track authorisation, etc.)
- Prior authorisation in specific cases
- Stronger inspection powers, and real sanction powers

⇒ Rationale in the law : streamlining notification requirements & developing a consistent enforcement policy

⇒ We are also developing a stronger communications policy

CNIL's inspection powers reinforced

- Possibility to have access to all professional premises
- Possibility to request all necessary documents and to take a copy, to have access to all IT systems and to request transcription of the data

But :

- Only a doctor may access health data
- Files on the security of State may, under certain conditions, not be subject to these checks

Relevant facts and figures

- 2001: 14 inspections
- 2006: 127 inspections

Prominent cases for 2006/2007:

- Major inspection programme in the context of the setting up of the DMP (the French eHR)
- « Navigo » scheme (e-ticketing application in the Paris network of public transportation)
- Joint action CNIL/HALDE (compliance with data protection and anti-discrimination laws)

Assessment of CNIL's inspection policy

- Inspections now have a major role in CNIL's global policy
- An important factor of credibility
 - But more staff needed to meet expectations
- One small inspection can have big consequences
 - Ex: inspection at one hotel => the group has launched a worldwide audit on its data protection practices
- Direct link to sanctions powers and policy

Sanctions : what can CNIL do? (1)

- Warning (“*avertissement*”)
- Compliance order (“*mise en demeure*”)

If non compliance with such an order:

- Financial sanctions (except State):
 - up to 150.000€
 - if subsequent offence : 300.000€ or 5 % of turnover (max 300.000€)
- Issuance of order to stop processing

Sanctions : what can CNIL do? (2)

- In case of emergency:
 - interruption of processing (3 months max.),
 - blocking of data (3 months max.)
 - Information of Prime minister if public security file involved
- If particularly serious offence, President can ask the judge to order any necessary security measure
- Withdrawal of authorisation
- Possibility to refer cases to the Public Prosecutor (not a sanction as such) : sanctions up to 5 years imprisonment and 300.000€
- Sanctions may be appealed to the Council of State

Sanctions: how does it work?

- Creation of a specific committee by the law: the « restricted committee » (« *formation restreinte* »)
 - Composed of President, 2 VPs, 3 members elected by Commissioners among themselves
 - The only competent organisation within CNIL to impose warnings and financial sanctions (not other sanctions)
 - In case of emergency, same sanctions may be imposed by President + VPs (« bureau »)
- In operation since January 2005
- Since Sept. 2004: « Sanction Unit » created on CNIL's staff to feed the agenda of the restricted committee
- Many formal rules of procedure need to be followed to ensure due process

A few figures since January 2005

148 procedures

- 126 “compliance orders” (« mises en demeure »)
- 15 financial sanctions
- 9 injunctions to put an end to a processing (ex: no more use of non “opt-in” files for commercial and political emailing)
- 14 warnings

Financial sanctions: 228.300€ in total

- Crédit Lyonnais: 45.000€
- Isorama: 60.000€
- Tyco Healthcare: 30.000€
- Crédit Agricole Centre France: 20.000€

Sanctions – the good sides for CNIL

- Compensates the lack of enforcement of DP issues in the courts for want of time, resources, and DP awareness (e.g. on spam)
- Some cases would not be dealt with otherwise (issues of costs, length of judicial procedures, etc)
- Helps being taken seriously by data controllers
- Great medium for communications and awareness raising
- Has raised the level of responsibility within data controllers' organisations where data protection issues are dealt with

We would never go back!

Sanctions – the other side

Imposing sanctions is no easy decision to take:

- Heavy consequences for controllers
- Need to ensure consistency between cases, and proportionality : risks for the image of DPAs too!

*It is a power to use with courage, confidence
but utmost care*

Impact on methodology and procedures

- A real enforcement policy dramatically changes the way CNIL used to work
 - Formalism, strict procedures, etc.
- It has an impact on all the other aspects of CNIL's work
 - E.g. notification, communication, complaints, etc.: need to develop a *horizontal way of thinking* in the organisation

Impact on internal organisation

- Creation of a dedicated inspection department (2001) and of sanction unit (2004)
- Specific requirements in terms of staffing (e.g. for inspections: former policeman; mix of lawyers and IT experts)
- Necessary to ensure good coordination with other departments (legal; complaints) to detect cases for inspections & sanctions and to set up a yearly policy – requires building horizontal thinking
- A reorganisation is pending to ensure the proper implementation of these policies

Some interrogations in terms of strategy

- What sectors of activity should be concerned by inspections and sanctions?
- Should a distinction not be made between failure to comply with essential or formal requirements (eg breach of access right v. no notification)?
- When is a warning an adequate sanction; when should we rather use compliance orders?
- How to ensure consistency between decisions to apply sanctions ourselves and decisions to refer cases to court?
 - Which relations with the Public Prosecutor's Office?
- What are the relevant criteria to set the level of a fine? ...

Some shortcomings in the law

- Main sanctions powers (ie injunction to put an end to the processing and financial sanctions) must always be preceded by a compliance order
 - May hinder the effectiveness of CNIL's powers
- Maximum amount of 300.000€ should be increased (not sufficient for big data controllers)
- No financial sanctions against controllers in the public sector : questionable under circumstances
- Difficult in practice to publish decisions (yet « naming and shaming » is very efficient)

We will ask for change when time is ripe

Commission nationale de l'informatique et des libertés

8, rue Vivienne

CS 30223

75083 PARIS cedex 02

Tel : 00 33 1 53 73 22 22

<http://www.cnil.fr>