

Data Protection Conference 2009: “Personal data – more use, more protection?”
European Commission, Brussels, 20 May 2009

“Transparency and Notification in the Age of Internet – Some Thoughts on the Need for More Effective Protection in Practice”

Peter Hustinx

European Data Protection Supervisor

I welcome this opportunity to contribute to this conference on new challenges for privacy and personal data protection, and on how data protection should face these challenges and be more effective in practice.

Transparency has always been a key principle of data protection. Fair and lawful data processing requires that data subjects are sufficiently aware of what happens to their data so as to be able to exercise their rights. The general public should also have adequate means to verify what is happening. This means that transparency is also an important tool to ensure compliance with data protection rules and principles. The notification of processing operations to supervisory authorities and their publication in a public register should of course be seen against the same background.

I would like to focus today on *four* different dimensions of the transparency principle and see how they could help to make data protection more effective in practice.

The *first dimension* is often overlooked, since it is so implicit in the present legal arrangements: i.e. the fact that the responsibility for compliance with data protection rules lies with the controller. How this responsibility is organised and executed in practice has been left open, except for the rules to be complied with and the liability and sanctions for infringements.

However, recent experience with data breaches, not only in the UK but also in other Member States, strongly suggests that internal arrangements for data governance and

accountability are often far less developed or less effective than might be expected. Top level management is often not sufficiently aware of data processing practices in their own organisation and therefore not able to influence what is happening. In other words: a clear lack of transparency and control *inside* responsible organisations.

It would be important to develop incentives for an improvement of this situation. One option is to build on the trend towards mandatory security breach notifications – first in the e-Privacy Directive, later more generally. Another option is already available in the general language of Article 17 of the Data Protection Directive: “the controller must implement *appropriate technical and organizational measures* to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, (...) and *against all other unlawful forms of processing.*” This goes in fact far beyond traditional security measures and might also involve internal management arrangements, depending on the risks at stake.

Of course, any standards for data governance and accountability should be scalable and take account of the circumstances of each case. But inadequate arrangements could be a source of liability and attract the attention and intervention of regulators.

The *second dimension* of transparency is that data subjects are sufficiently informed about the collection and use of their personal data. Articles 10 and 11 of the Data Protection Directive lay down a number of requirements, depending on whether data are collected from the data subject or obtained otherwise. It is clear from these provisions that they are designed to guarantee fair processing having regard to the specific circumstances of the case. These obligations are therefore ‘not cast in stone’ and do not apply where the data subject has already been informed.

There are some obvious ways to ensure sufficient transparency for data subjects and avoid a situation of unhelpful notices or ‘notice fatigue’. The first option is to build on the *exceptions* and ensure that all relevant information has *already* been provided at the most appropriate moment. This leads to better information and more transparency. The second option is the use of *layered* notices that contain the main points and refer to other documents or websites for additional information. The Article 29 Working Party has issued useful guidance in this respect.

The *third dimension* of transparency is in relation to the supervisory authorities. The current legal framework relies for this purpose to a large extent on the obligation to notify individual processing operations to an authority (see Articles 18-21 of the Data Protection Directive).

A somewhat closer look at these provisions reveals that they are based on a more selective and risk based approach than many critical observers are aware of. There is in fact a distinction in three categories:

1. prior checking in cases of *specific risks*, as defined by national law;
2. exemption or simplification of notification, where the rights and freedoms of data subjects are *unlikely to be adversely affected*;
3. notification only where the other options do not apply.

The second option of exemption or simplification has been used very unevenly in practice, as some Member States have large or general exemptions – on the basis of detailed rules or after appointment of a data protection officer – and other Member States have virtually none. This gave rise to significant differences in administrative burdens and to unequal outcomes in actual transparency of processing operations.

However, there is also increasing doubt whether notification of processing operations to a supervisory authority is the most appropriate way to ensure both transparency and effective supervision. It seems to me that there are sufficient reasons to look for better alternatives. These could consist of a baseline of simplified registration of *controllers* rather than processing operations, in combination with additional requirements in case of risks that the rights of data subjects might be adversely affected or where specific risks would be involved.

The question whether certain standards for data governance and accountability are complied with could be an element in this evaluation. This already applies to the appointment of data protection officers, but there are also other means to ensure more effective protection in practice, including those subject to third party verification and additional transparency, like privacy seals, privacy audits and privacy certification.

None of these approaches would of course prevent an inspection by a supervisory authority for appropriate reasons or sanctions being imposed in case of infringements. A simplification of notification and flexibility for other means of accountability should in my view go together with stronger powers for supervisory authorities and more effective sanctions.

The *fourth dimension* of transparency involves the general public and has already been mentioned in passing. In short, public registers are now not always available, often incomplete and sometimes unduly detailed. All this may lead to obvious deficiencies that justify a fresh look on the matter. However, it should always be possible to receive information from the controller, and transparency of processing operations should be a basic element of public accountability.

In fact, it would be a good idea in my view to ensure that a statement of assurance on an organisation's data protection performance is made part of its standard reporting obligations, so that both supervisory authorities and the general public, including any special stakeholders, could verify and where necessary challenge that information. This might also stimulate helpful competition in privacy relevant services or products.

I think this approach would be fully appropriate for important players, public or private, either on-line or off-line, and could be replaced by less demanding solutions for small and medium sized organisations. However, overall, it would lead to a far more effective system of checks and balances, in which controllers and regulators can focus on the most important issues and substantive needs for effective protection in practice.

I hope that these brief remarks are helpful in stimulating ideas and further discussion, which are no doubt both necessary. I shall look forward to this discussion, today and in the near future, with the utmost interest.