

**3<sup>rd</sup> International conference on Computers, Privacy & Data Protection: An element of choice**  
**30 January 2010**

**Panel 8 – Revising the Directive: Experts’ Perspective**

**Intervention by Jacob Kohnstamm**

Dear friends and colleagues,

It is an honour for me to speak once more at this yearly event, a European conference that unites the best and brightest experts on data protection.

In my intervention, I will be “going Dutch”. No, not in the sense of this expression, but in the sense of “talking like a Dutch uncle”, in other words, being rather to the point and quite blunt. Today I would like to do great injustice to the work of the Article 29 Working Party, the independent EU advisory body uniting all EU Data Protection Authorities: I want to discuss with you only a small selection of the very extensive, robust and elaborate advice to the European Commission on the future of privacy, developed by the Working Party. Moreover, I will provide you with my own interpretation of the Working Party view.

I would like to focus on the roles that the various actors involved in data protection, namely the data subject, the controller and the Data Protection Authority, should play. In light of the challenges ahead of us, technological changes and globalisation, the legislator should define much more sharply the role each actor must be playing. This will strengthen the role of each, and thereby strengthen the functioning of data protection. What do I envisage?

**First, the data subject:**

It is indispensable that the position of the data subject in the data protection framework is strengthened. Through empowerment of the data subject, he can choose to play a more active role in the protection of his personal data. The importance of this shows from a research that the Dutch DPA undertook in the context of last year’s data protection day: People who start from the basic assumption « I have nothing to hide, so ‘they’ are allowed to know everything about me » were confronted with concrete examples of invasive data procesings that would affect them. These persons showed a double reaction: On the one hand, they showed great concern, even panic, upon the daunting realisation of what is done to their personal data. But, on the other hand, immediately upon that, they showed resignation: People take these processings of personal data as a fact of life, against which nothing can be undertaken, unless one is willing to live as a hermit and be cut off from modern daily life. This reaction to a great extent explains why the exercise of individual rights and the amount of court cases is so low: Not because people do not care, but because they think it will not make a difference.

Therefore, empowerment of the data subject requires first and foremost more **transparency**. Citizens should be informed in an understandable and easily accessible manner about the purpose

of a processing, by whom this is undertaken and on what grounds. The current duty to inform data subjects is not always properly put into practice. A new legal framework should provide alternative solutions, in order to enhance transparency.

Secondly, empowerment of the data subject entails giving him more feasible choices to **execute and exercise his rights**. In particular, the possibility of **class actions** before the court should be introduced into the Data Protection Directive. This is crucial, because court proceedings can sometimes be very difficult and costly, and, because the Data Protection Authority should no longer be the primary organisation handling individual complaints.

Third, controllers should provide data subjects with more easily accessible, more effective and affordable **complaints procedures**. If these do not resolve the data subject's complaint, the data subject should have the choice to go to an alternative dispute resolution procedure. These options should also be included in the new legislative framework.

As to the second group of actors, the **data controllers**, what should be their role? We consider that bureaucratic burdens such as notification should be limited, and that supervision must shift from an ex-ante to an ex-post approach – an issue to which I turn hereafter. As a consequence, more freedom is provided to the data controller. However, more freedom also comes with more responsibility:

Data controllers are the primary actors responsible for **compliance**: They have to ensure that they observe in practice the substantive principles and obligations laid down in the law, and that they are able to do so.

Secondly, controllers should have the necessary internal mechanisms in place to be able to actively **demonstrate compliance** to relevant stakeholders, including national DPAs: In other words, they have to be **accountable**. The Working Party therefore considers that the introduction of the **accountability principle** into the new comprehensive framework is essential.

Thirdly, we have to **move away from** a strong reliance on **consent**. In a digital world which, due to technological innovations and innovative forms of collaboration between parties, becomes ever more complex for average citizens to grasp, consent alone becomes ever more meaningless: In a digital world, people do not always oversee what they consent to, in spite of - or is it because of - elaborate information notices, people have no idea of the consequences of refusing consent, and they do not know whether they have a real alternative. This implies that compliance and accountability are far more important: data controllers should have the internal mechanisms in place to be able to both **ensure** and actively **demonstrate compliance**. What do I think of concretely ?

1. A more effective implementation of the transparency obligation, via – understandable – privacy policies
2. Easily accessible complaints procedures for citizens
3. The obligation of a privacy breach notification
4. Carrying out Privacy Impact Assessments, in particular for data processings presenting a significant risk to the rights and freedoms of individuals

5. Real accountability: Ensuring execution of policies, and possibility for internal and external verification, remediation and enforcement.

Taken together, such a framework that is less prescriptive beforehand, and focuses more on « data protection output » by the controller, at the same time requires a shifted role for the **third** category of actors, the **Data Protection Authorities**. Data Protection Authorities, should, to quote a distinguished colleague of ours, present here today, « be selective to be effective ». The Supervisory Authority should be strong and bold, and focus much more heavily than today on its primary activity: Independent supervision. In the face of globalisation, stronger supervision is necessary not only at national level, but also at EU level. This could be by providing the Article 29 Working Party with supervisory powers, or through other mechanisms.

Independent strong and bold supervision means that it is indispensable that DPAs are able to fix their own agenda when setting priorities. In my view, the **DPA no longer is the primary agency to handle individual complaints**. **Neither** should it provide **individual advise** to data controllers, as this could conflict with its role as an independent enforcement agency.

The only **advisory role** all DPAs must play is in the **legislation making process**. This is essential, because the knowledge that DPAs acquire from investigation and enforcement actions often is necessary to improve legislation. In addition, the new framework should ensure that DPAs have an advisory role towards their national parliaments and/ or other competent national institutions, at the time when these are involved in the drafting process of new EU legislation.

Strong and bold supervision also implies that the **enforcement role** of DPAs needs to become **increasingly important**. This requires more harmonised and specific supervisory powers for DPAs than is currently provided for in the Directive. Amongst others, DPAs should have the power to impose substantial **financial sanctions**.

And finally, you will not be surprised to hear that I consider that **DPAs need more staff** and more funding to be able to fulfill their new, strengthened, supervisory and enforcement role.

Dear friends and esteemed colleagues, with the reinforcement of the roles of these three groups of actors, I trust that data protection will become stronger in the future. I hope you have enjoyed this « Dutch treat », and that it will find its way into our European deliberations on the future of privacy. Thank you for your attention.