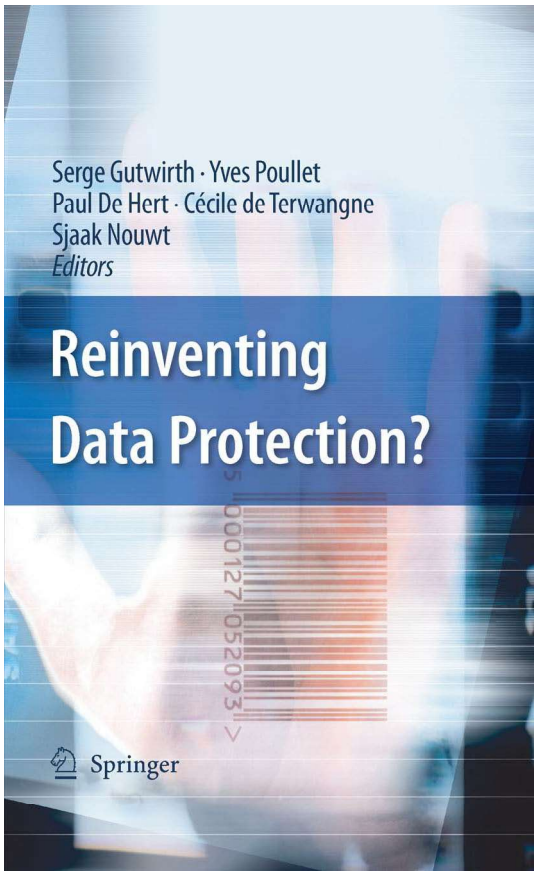
Serge Gutwirth · Yves Poullet
Paul De Hert · Cécile de Terwangne
Sjaak Nouwt
Editors
Reinventing
Data Protection?
Springer

Reinventing Data Protection?

Serge Gutwirth · Yves Poullet · Paul De Hert ·
Cécile de Terwangne · Sjaak Nouwt
Editors

Reinventing Data Protection?

Springer

Editors
Prof. Serge Gutwirth
Vrije Universiteit Brussel
Center for Law, Science
Technology & Society Studies (LSTS)
Pleinlaan 2
1050 Brussel
Belgium
serge.gutwirth@vub.ac.be

Prof. Yves Poullet
University of Namur
Research Centre for Information
Technology & Law
Rempart de la Vierge 5
5000 Namur
Belgium
yves.poullet@fundp.ac.be

Prof. Paul De Hert
Vrije Universiteit Brussel
Center for Law, Science
Technology & Society Studies (LSTS)
Pleinlaan 2
1050 Brussel
Belgium
paul.de.hert@vub.ac.be

Prof. Cécile de Terwangne
University of Namur
Research Centre for Information
Technology & Law
Rempart de la Vierge 5
5000 Namur
Belgium
cecile.deterwangne@fundp.ac.be

Dr. Sjaak Nouwt
Royal Dutch Medical Association (KNMG)
Mercatorlaan 1200
3528 BL Utrecht
Netherlands
s.nouwt@fed.knmg.nl
(formerly: TILT, Tilburg University, Netherlands)

ISBN 978-1-4020-9497-2 e-ISBN 978-1-4020-9498-9

DOI 10.1007/978-1-4020-9498-9

Library of Congress Control Number: 2009920948

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Chapter 7
The Role of Data Protection Authorities

Peter Hustinx

7.1 Introduction

I am delighted to deliver this contribution about the role of data protection authorities (DPAs) and let me be very clear at the outset about my main message.

The title of my speech in the initial draft programme was: 'Do we need data protection authorities?'. My answer to this more challenging question is not simply 'yes' but rather 'YES, BUT'. In other words, a positive answer with two important conditions:

1. within a legal framework that allows them to be effective,
2. with a strategic approach and the ability to make a difference.

I am here in good company: Article 8.3 of the EU Charter of Fundamental Rights, which has now become a binding element of the Reform Treaty, provides that 'compliance with data protection rules shall be subject to control by an independent authority'. Recently, the Declaration of Civil Society Organisations, adopted on 25 September 2007 in Montreal, stated that 'stronger, more aggressive action by privacy commissioners is required', finding them 'uniquely positioned to defend our society's core values and rights of privacy'.

The existence of DPAs has been a typical feature of European data protection law since its inception but the reasons for their establishment have not always been clearly articulated and it has also taken some time before this element developed into a constitutional principle.

Taking a closer look at the reasons underlying their establishment can help to better appreciate the role of these bodies and to understand why they are now widely considered as a key element of the privacy landscape. Such an analysis is also important to find ways that help them to develop their role and to enhance their effectiveness.

P. Hustinx (✉)
European Data Protection Supervisor (EDPS), Brussels, Belgium
e-mail: edps@edps.europa.eu

S. Gutwirth et al. (eds.), *Reinventing Data Protection?*

DOI 10.1007/978-1-4020-9498-9_7,

7.2 Historic Background

In retrospect, it is surprising to see that, in spite of experience developed in Germany, Sweden and France, the concept of a 'data protection authority' played only a very limited role in the Convention on Data Protection, also known as Convention 108 of the Council of Europe, when it was concluded in 1981.

The central obligation of each Party in Article 4 is to take 'the necessary measures in its domestic law to give effect to the basic principles for data protection' set out in the Convention. Article 10 provides that each Party must establish 'appropriate sanctions and remedies' for violations of these basic principles. The explanatory report clearly mentions the need to guarantee '*effective protection*' but leaves the way in which this should happen for each Party to decide. The existence of supervisory authorities is only mentioned as a feature of national laws. The original drafters of the Convention were obviously reluctant to impose this on all Parties as a basic legal requirement.

This situation changed with the adoption of the European Data Protection Directive 95/46, which took the Council of Europe Convention as a starting point but specified it and added to it in many ways. Article 28 of the Directive introduced an obligation for each Member State to have a supervisory authority responsible for ensuring compliance, and 'acting with complete independence'. Recital 62 of the preamble underlined that 'the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data'.

The words '*acting* with complete independence' were a compromise formula, chosen to ensure some flexibility but it is hard to see how 'complete independence' could exist without sufficient institutional safeguards in place. This issue is highly relevant in a case presently before the European Commission and involving Germany, which is likely to end up before the Court of Justice in the near future.

Article 28 of the Directive also provides that supervisory authorities should have certain powers, such as consultative powers, investigative powers, effective powers of intervention, the power to engage in legal proceedings or bring violations to the attention of judicial authorities, to deal with complaints, etc. This seems to assure them a central position. However, they never decide in last resort and their decisions may be appealed to the courts.

The adoption of the Directive has led to an Additional Protocol to Convention 108, which basically takes up all elements of Article 28 of the Directive. The preamble of this Additional Protocol clearly states that 'supervisory authorities, exercising their functions in complete independence, are an element of the effective protection of individuals with regard to the processing of personal data.' The explanatory report even concludes that data protection supervisory authorities 'have become an essential component of the data protection supervisory system in a democratic society.' This report also puts a lot of emphasis on the notion of 'effective protection' and the role of supervisory authorities in ensuring it.

This trend is finally also visible in Article 8 of the European Charter of Fundamental Rights, which has now been made binding in the Reform Treaty. Article 8 has recognized the protection of personal data as a separate fundamental right. Its third paragraph – as already mentioned – provides for control by an independent authority.

This all means that the principle of 'independent supervision' and the existence of 'independent supervisory authorities' have developed, at least at the European level, into a constitutional element of the right to data protection in a democratic society. This seems to be based on their primary mission to 'ensure compliance' and is closely linked to the notion of 'effective protection'. This also means that it is crucial for independent supervisory authorities to regularly think about their own effectiveness and to consider ways to measure and where necessary improve their performance.

7.3 Further Analysis

It is probably only fair to say that this approach was facilitated by the fact that all 'early starters' in Europe and subsequently all Council of Europe and EU Member States, were dealing with 'data protection' as *an issue of general and structural importance for a modern society* and therefore typically opted for a general legal framework with a wide scope, including both public and private sectors and hence virtually all relevant areas of society (often referred to as the 'omnibus approach').

Such frameworks usually consisted in a mix of substantive rules, individual rights and formal procedures, to allow a step-by-step – and where necessary differentiated – implementation in the various sectors of society, to respond to the characteristics and specific needs of those areas or their special fields of interest. Since no other public authority was in the position to follow this development and to ensure a consistent approach, this task was given to 'data protection authorities', which were established for this purpose. This decision should of course also be understood in the light of social and political preferences in Europe to see a *public authority* deal with this task.

It is tempting to also point at the fact that 'data protection' developed in Europe in the context of human rights was recognized as a *fundamental right* of its own. The truth is however that no other fundamental right – except the right to a fair trial – is structurally associated with the role of an independent body to ensure its respect and further development. This right is special in the sense that it is considered to be in need of '*structural support*' through the establishment of an independent authority with adequate powers and resources.

Certain other fundamental rights, such as the freedom of expression and the freedom of assembly and association, already have strong institutional stakeholders, such as the media, labour unions or political parties but that is not the case for data protection. Most of what is happening in this area is moreover invisible and often difficult to understand or deal with without technical expertise. That

explains the general trend to charge an independent authority with the task to address these issues.

It is also useful to consider *what might have been alternative approaches*. The first and perhaps most obvious alternative would have been to limit data protection law to sets of rights and obligations and to leave conflict resolution to *existing mechanisms, such as the court system and civil procedure*. However, this would have had at least three negative consequences. Firstly, it would have put most 'right holders' in a very difficult position, left alone with the 'onus of initiative', without adequate expertise and with a very uneven distribution of interests, mostly limited at the individual side and typically rather large at the data user's end. Secondly, as a result, it would have taken a long time before the meaning of legal norms would have become sufficiently clear to have any preventive impact. Thirdly, the consistency of this impact in various sectors would have been dubious and unpredictable and the value of data protection as a fundamental right would have suffered considerably as a result.

The same would apply to most common procedures in *administrative law* and more so since these procedures typically deal with administrative 'decisions', directly affecting the individual, rather than with processing of personal data, which may or may not be at the basis of such a decision. An independent public authority was therefore in a much better position to protect the interests of individual right holders in a consistent way and to strike a fair balance with other private or public interests, where necessary.

Relying on the *criminal law* as yet another alternative, would have been hardly more attractive. Firstly, in short, the use of criminal law requires clear and precise legal norms but these are mostly not available in data protection, except in special fields. Secondly, violations of data protection provisions would have to compete in practice with other types of simple or complicated 'ordinary crime' and it would be unlikely that enforcement of data protection law would have a high priority on the list. The lack of expertise to deal with these matters in an integrated fashion would in any case have led to unsatisfactory results. As a result, criminal law has played only a limited role as 'back up' for enforcement in special cases.

It is therefore not surprising that national law mostly opted for an approach '*sui generis*' involving a data protection authority with a specific mandate and a special position, since it had to deal with other parts of government as well as with various private parties and interests. These authorities were given a wide responsibility to deal with all relevant issues in an integrated manner and thus also to 'generate' guidelines for other parties to work with, to raise awareness of data protection and to act as a 'focal point' in the public debate.

7.4 Different Experience

As to the precise mandate of these authorities, different models have been used in various Member States for a long time. The original approach in Sweden was based on the general need for a license. The French approach was far more selective and

the German approach provided for monitoring on an *ex post* basis and powers to make recommendations rather than binding decisions. The Data Protection Directive has harmonised the roles and powers of supervisory authorities to a large extent, while adding that they must exercise their functions 'in complete independence'. However, the Directive has also introduced a few other interesting developments.

Firstly, it is evident that the Directive has encouraged a more *selective approach to supervision*, which allows a distinction between relevant cases on the basis of the risks that are involved. Only those cases likely to present specific risks are subject to prior checking by the supervisory authority. This applies regardless of the sector involved but the national law can determine which systems are considered to present specific risks.

Other systems are subject to prior notification to the supervisory authority but the Directive allows important exceptions to this principle. The possibility to develop exemptions for certain categories that do not present any risks, provided that some conditions are fulfilled, is clearly based on the experience in certain countries with similar exemptions (e.g., France and the Netherlands).

The second option – which provides for the appointment of an *internal privacy officer* – is even more interesting. This option has now been adopted in different countries following positive experiences in Germany. On the European level, there is a general obligation for Community institutions and bodies to have at least one data protection officer, with a number of specific tasks. Together, they are a valuable network of 'first line' experience, with which my office cooperates on an almost daily basis.

This can also be understood as a first important step to come to a better *distribution of roles* in data protection that allows independent authorities to concentrate on larger or more strategic issues.

In a general way, the Directive also encourages the development of *codes of conduct* for different social or economic sectors. These different instruments are designed to encourage a development in which other actors can take responsibility for an effective integration of data protection rules and principles in the normal practices of relevant organisations. Data protection is also – and not least of all – an important part of good quality where services are delivered with electronic means.

As to the relations with data subjects, the first goal for supervisory authorities should be to *raise awareness* and to *enable them to exercise their own rights*. If they do, this will gradually also encourage responsible controllers to invest more in their relations with data subjects. Investing in awareness of both controllers and data subjects is thus also a good strategy for supervisory authorities.

In my previous role as data protection commissioner in the Netherlands, I have had some valuable experience with the involvement of *intermediary organisations*, like consumer unions, trade unions, etc. The latter were quite active with data protection in employment. Under national law, these organisations also had a right to initiate legal actions in the interest of their members.

For supervisory authorities this implies a rather *complex environment* of different sectors with different needs and requirements. Independent authorities should in my view not refrain from entering into appropriate and productive relationships with

these *different stakeholders*. To the contrary, many colleagues have discovered the need for partners and allies in the execution of their role and some of them have been very successful in that respect.

7.5 More Effectiveness

This overview should also deal with the question whether there are certain areas where the current role of data protection authorities might be subject to improvement in order to make their work more effective. This is an important question, since the primary mission of data protection authorities is to ensure *compliance* and to promote *effective protection*. It is *only* through these concepts that data protection rules and principles can become a reality in practice.

As a first point of attention, I would like to mention that data protection authorities should have the *possibility to set priorities* and concentrate on issues of special importance or posing special risks. Many authorities presently suffer because their activities are dominated by individual complaints. This may have different reasons but they tend to reinforce each other and limit the capacity of the authority to invest sufficient resources in important issues: firstly, a lack of alternatives for enforcement of rights by data subjects and secondly, a lack of possibility for authorities to set their own priorities and to make selections.

An efficient data protection system should allow data subjects to exercise their rights directly with responsible controllers and in case of problems choose from different alternatives for appropriate follow up. Among these alternatives, seeking help from a data protection authority would certainly be a necessary option but it should neither be the *only* one, nor a *compulsory* step before taking further legal action. Otherwise, the data protection authority would be in the position of a monopolist or develop into a bottleneck and probably both.

This would be more regrettable if the data protection authority would be obliged to deal with all complaints and requests for assistance in a similar fashion, without the possibility to exercise a reasonable discretion as to whether and how to deal with the matter. This may be a common approach for courts and understandable from the point of view of general administrative law but for data protection authorities with wide responsibilities and always limited resources, it only means that individual cases will dominate the agenda at the expense of other matters.

The appropriate remedy for these problems should thus be twofold: firstly, encourage *alternative courses of action* for enforcement of data protection rights and, secondly, make sure that data protection authorities are able to set *priorities* and develop more *flexible methods* of dealing with individual complaints, including simple procedures and using them in support of *ex officio* inquiries against responsible parties.

As to alternative courses of action, it seems appropriate to also consider introducing the possibility of *class actions*, empowering groups of citizens to jointly use litigation in matters concerning protection of personal data, as well as actions,

initiated by legal persons whose activities are designed to protect the interests of certain categories of persons, such as consumer associations and trade unions. Both might be a powerful tool to facilitate the enforcement of data protection law in various situations.

It might also be interesting, in combination with these two solutions, to provide for simple ways of dealing with signals that data protection rules are being breached, without necessarily going into the details of every single case. It goes without saying that standard procedures for enforcement of data subjects' rights should be as simple as possible and should provide access to data subjects without undue formalities.

Finally, it would be interesting to invest in different means that enable organisations to *demonstrate* that 'privacy and data protection' matter for them and to use them for competition in the market. This might work in the case of 'privacy seals' for privacy compliant products and services and for third-party 'privacy audits'. Both might be good examples of 'privacy relevant services' that could be effective *in addition* to the role of data protection authorities and should not necessarily be provided by them. It would be up to the authority to decide to what extent it would be prepared to rely on the result of those services in individual cases.

These and other ideas have been mentioned in my opinion of 25 July 2007 on a better implementation of Directive 95/46/EC and are also discussed in the context of the 'London Initiative', which was launched in November 2006 and involves the sharing of 'best practices' among supervisory authorities. There is still a lot to be done but these remarks are hopefully sufficient to explain why data protection authorities are a key element in the privacy landscape and how they could be more effective.