Peter J. Hustinx

Co-regulation or self-regulation by public and private bodies – the case of data protection

1. Introduction

In his whole career, Alfred Büllesbach has demonstrated a great capacity for combining or switching from different disciplines, social sectors, national environments and so on. In most of these situations, he not only demonstrated great skills in the subject at hand, but above all impressed observers with a unique combination of boundless energy and catching enthusiasm which has left its marks on all those who crossed his path. This seems to provide the ideal inspiration for a reflexion on one of the areas he has been active in – i.e. data protection from an international and cross-sectoral point of view, but with a solid base. In this case, the solid base is in the Netherlands and the question was how to develop a combination of means to improve the effectiveness of data protection.

This article sets out to present the main lines of the constitutional framework within which »data protection« or the protection of personal data has developed in the Netherlands. Against this background, it discusses the reasons why and the different ways in which self-regulation has played its role in that development. The article then focuses on the structure of the Data Protection Act and on the ways in which the Data Protection Authority has interpreted its role in that context and is planning to proceed in the near future.

2. Constitutional framework

It should be realised at the start that the Netherlands has traditionally been very open minded towards international law and legal developments in the international scene. Article 93 of the Dutch Constitution provides that terms of international agreements which can be applied directly, have such binding force after the publication. Article 94 of the Constitution provides that where the application of a certain legal provision would be incompatible with a binding provision of an international agreement, the latter must always prevail. In legal and political discussions on privacy and data protection, this has resulted in an early and frequent use of Article 8 of the European Convention on Human Rights (ECHR):

Article 8

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Although the precise scope of the right to privacy as described here is still uncertain, there can be no doubt that it at least covers information of a more sensitive or intimate nature. This implies that any interference by a public authority is only allowed under the conditions laid down in the second paragraph. Any such interference should be »in accordance with the law« and should also be »necessary in a democratic society« for certain purposes. In its case law, the European Court of Human Rights has developed criteria for the quality of national laws and the need to provide for certain measures. The latter should be »proportional« to a pressing social need and where necessary accompanied by »additional safeguards« against abuse. In addition to the »negative« protection against undue interference by public authorities, the Court has developed the idea that there is also a »positive« obligation to provide a sufficient legal protection against undue interference by others.

In the early 1970's the Council of Europe came to the conclusion, that Article 8 ECHR had a number of defects in the light of new developments, particularly in the area of information technology. The uncertain scope of the term »private life« could create problems where the information was less sensitive. The limitation to »public authorities« seemed to overlook the possibility of interference by »private interests«. It was also felt that more positive action was required. This resulted in 1981 in the adoption of the Convention on Data Protection, laying down the basic principles for data protection, which later served as the conceptual starting point for Directive 95/46/EC, now the dominant instrument in this area.

Article 10 of the Dutch Constitution, adopted in 1983, carefully reflects this development. The first paragraph provides for a right of everyone to respect for his privacy, subject to restrictions provided in or by virtue of an Act of Parliament. This latter element is somewhat stricter than Article 8 ECHR which applies in other respects. The second and third paragraph of Article 10 provide for further safeguards for the protection of privacy with regard to the processing of personal data. These provisions are still at the basis of the national legislation which now implements the Directive.

3. The role of self-regulation

It is often overlooked that »self-regulation« is nothing new, but actually nothing more or less than the »default position« of the way in which most problems are solved in an orderly society. If legislation or other forces do not intervene, it is self-regulation by which individuals and organisations handle their interests.

In discussions about privacy and data protection, the concept of »self-regulation« has also been used in a more strategic way. Initially, the possibility of self-regulation is often advanced as a means of preventing or postponing legislation. In a more positive sense, self-regulation can be used as a means to experiment and to prepare for legislation in a flexible way. A third option is that self-regulation serves as a sector-specific way to implement legislation and to avoid too much detail in the legislation itself. A fourth option is that self-regulation can serve as a way to provide solutions beyond the scope of the existing legislation, which may or may not result in a new cycle of policy-making along the lines mentioned before.

When a Dutch Royal Commission reported on the need for data protection legislation in the mid 1970's, it suggested that self-regulation should play its part, at least during the long phase in which this legislation was to be developed. In retrospect, the commission could hardly have been more right. It took almost fifteen years and three draft bills, before the Data Protection Act of 1988 was finally adopted. Most of this long period was spent on »methods« rather than on »substance«: the question how data protection law could be made effective without much bureaucracy. By the time the legislation was adopted, self-regulation in various sectors and on different levels of government had developed into a standard practice, both in the public and in the private sector.

The Data Protection Act took this on board in two ways. On sector level the Act provided for the possibility to develop a code of conduct as means of implementation and to request the Data Protection Authority for its approval. The decision of the authority was non-binding, but in practice often seen as a seal of good quality. Under this regime, twelve codes of conduct have been officially approved, which covered major sectors like banking and insurance, direct marketing, health and pharmaceutical research. The relevant provision of the Act served as a model for Article 27 of Directive 95/46/EC, which provides for implementation via sectoral codes of conduct, both on the national and on the European level.

The Data Protection Act also provided for regulations on an organisational level in the public sector. This feature did not return in the new Data Protection Act, which entered into force in September 2001. The sectoral codes of conduct still enjoy a considerable degree of popularity. Most of the existing codes are currently under revision for adaptation to the new legislation.

4. Data Protection Authority

The present Data Protection Act covers both the public and the private sectors, with only very few exceptions. Some specific areas, like the population files and the police, are covered by special legislation, which derogates from the general scheme. However, many other fields of activity are affected by legal provisions, which coincide with the general legislation and give it additional

substance. The implementation of the Directive required a general revision of this other legislation in order to make it fully compatible.

What resulted from this exercise is a mixture of continuity and change. The most important difference on a technical level is the replacement of the concept of »personal data file« by the »processing of personal data«. This shift is more in line with the development of technology, but also allows 'data processing' to be regulated more closely. Among the substantial changes are a greater emphasis on transparency, new rights for data subjects (i.a. right to object), and additional powers of enforcement for the Data Protection Authority. It now has the power to impose administrative fines, in cases of non-notification, and to exercise coercive measures in other cases of non-compliance. This second possibility is a last resort which may be necessary where data subjects or organisations acting on their behalf, like consumer or trade unions, do not reach an acceptable result.

Both in the previous and in the present Act, the Data Protection Authority has found itself competent to deal with a variety of tasks and subjects in an area which essentially covers all sectors of society, and certainly all those in the field of »information intensive services«. In order to invest its resources in the most productive way, the Authority has decided to structure its activities along four »policy tracks«: raising awareness, development of norms, information technology and enforcement. Together, these tracks can be regarded as a quality cycle which can be employed to enhance data protection in different sectors and individual organisations. In other words, it is a »strategic model« used by the Authority to develop its own policies and to measure the quality of data protection in organisations.

Different forms of communication are used to reach various »target groups« and to help raise their awareness of privacy issues. The Authority's website is the central part of its strategy which should allow individual organisations and intermediary organisations to find what they need to make informed choices on privacy related issues.

The development of norms takes place in preliminary surveys on different subjects, advice to government departments and parliamentary commissions on new legislation, discussions with various sectors of industry about new codes of conduct, and in formal decisions on individual cases about new or important questions. The result of this work is made available to the public and to interested organisations by means of different publications.

It is almost common place by now to say that information technology not only leads to new challenges for privacy and data protection, but also offers a number of solutions to solve or to reduce these problems. That is why the Authority made early investments in the development of Privacy Enhancing Technologies (PET) and is still making substantial efforts to promote the use of these technologies at the earliest possible stage. In this context, the emphasis is on »Privacy by Design«.

The final test of data protection is the degree in which it is followed in practice and enjoyed by data subjects. Privacy audits and other kinds of systema-

tic research are means to measure to what extent that goal is reached. Together with professional organisations and EDP audit firms, the Authority has developed standard tools to measure data protection compliance. The explicit aim of this project was to allow the »market« to provide and employ services which responsible organisations need to ensure compliance and which can also be built upon by the Authority. The new enforcement powers of the Authority only emphasized the need for this development.

The four »policy tracks« indicated here are developed in annual programs and evaluated on a permanent basis. Standard business is usually dealt with in a »front office« and special cases or projects are handled in the »back office«. The Authority reserves a certain part of its resources to deal with incoming requests and another part to initiate priorities of its own. No one should be surprised that »organisation and inspiration« go together, in this field as much as elsewhere.

5. Policy perspectives

In its latest policy plan, its first under the new Data Protection Act, the Authority has decided to continue and deepen its overall policy, which is based on an integrated approach of data protection, using all legal, technical and other appropriate means to ensure that the rights and freedoms of citizens in an information society are respected. However, the plan also contains some new elements which are relevant to the subject of this contribution.

The Authority emphasizes the responsibility of government and business for adequate data protection, as well as the right of data subjects to make the best use of their opportunities under the new Act. At the same time, data protection is perceived more and more as »critical success factor« for other important projects in our society, which range from e-government and e-health to e-commerce. Moreover, other organisations act as institutional safeguards in specific contexts, like consumer organisations and trade unions. The most effective policy for data protection authorities is therefore in many cases not to act directly, but rather to have other »stakeholders« act in the right direction. In this light, the Authority intends to emphasize its role as a 'second line' institution, whenever possible. In that capacity it will be in a better position to concentrate on subjects which require its primary attention and for which it has been given special powers and resources. What emerges is »co-regulation« with other players in the field of data protection. It is obvious that the Authority needs to be able to act and be both selective and flexible, in order to play its role in this context.

A second element in this approach is that the Authority will give more attention to various ways of systematic monitoring and is ready to enforce the law where that turns out to be necessary. This means a gradual shift to activities in the latter area and requires an internal separation of work in order to isolate education and consultancy from investigation and enforcement. The ideal

strategy would be to keep resources in the former area at the present level and to develop new resources in the latter. A »second line« institution should be in a position to deal with the more complicated questions that reach its desks. At the same time, the development of an adequate capacity for investigation and enforcement is crucial for the long term success of self-regulatory and co-regulatory approaches.

6. Final remarks

The primary purpose of this contribution is to give information about the way in which data protection has developed and is still developing in the Netherlands. A secondary purpose is to stimulate reflexion and discussion on a question that should permanently »bother« all data protection authorities: i.e. how to be most effective.

Other data protection authorities will have their own experience. However, it is quite clear that all of them are heading for »even more interesting times«. Exchanges of experience and co-operation between offices will be necessary as never before.