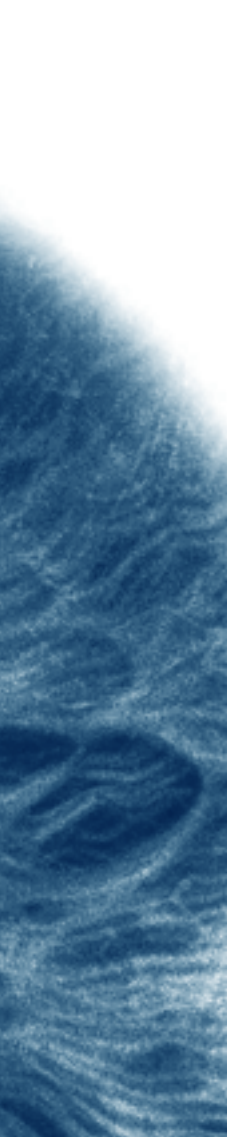




Trust

Trust stimulates social cohesion in society, acts as a lubricant in the economic engine and is vital for constructive and creative human relations. Trust is part of the social capital of the democratic constitutional state.

The objective of the WBP [Dutch Data Protection Act] is to make a contribution to the trust civilians can have in the way society handles personal data. Research carried out in 2004 and 2005 by order of the Dutch Data Protection Authority (Dutch DPA) demonstrates that this trust among citizens leaves much to be desired and in any case falls short of the importance they attach to a careful handling of their data in the various social domains.



Mutual trust and trust in society is created where the exercise of power in a democratic society is perceptibly and noticeably contained. Within that framework the WBP first and foremost fulfils a preventative role. Public and private powers, which are exercised partly on the basis of the use of personal data and which can negatively affect the development of an individual, must be contained. In order to protect privacy, the law therefore bans the unnecessary processing of personal data and further requires that personal data is handled in a considerate and proper manner.

Within the current social context there is a tendency to abandon the, until recently common, general attitude of trust in participants in social and economic life. The decline in social control, which for instance was still present in our society that was compartmentalized along socio-political lines, requires alternative management mechanisms. The large-scale automation and linking of files by the government and the business sector relates to this. Preventing the abuse of government provisions in an administrative-technical manner, increasing customer-orientation among the government and business sector and stimulating safety by strengthening the judiciary and police (powers) are high on the social and political agenda. Making the best possible use of the powers of technology is pursued here.

As a result, however, important social concepts are put under pressure. Three well-known fields in our legal system are the proportional application of control and investigative powers: the basic principle is trust, subsequently followed by a general supervision system and concluded by the investigation of offences in the event of reasonable suspicion. However, powers and means are more and more used at an early stage, whereas they were initially granted to be used in the event of activities aimed at repression. The obligation to store telecommunications data for the judiciary and police, preventative monitoring as to who enter and leave the major cities (the so-called virtual moat), the acceptance of extensive whistle blower and telltale provisions and the extensive check of all sorts of data prior to deciding to grant benefits are manifestations thereof.

Outside the field of investigation and prosecution too, government institutions and private corporations create files at an early stage and install links with a view to preventing any conceivable future abuse. The development of the 'alternative government', which wants to 'serve' citizens proactively, creates new possibilities and dependencies for that. Slightly exaggeratedly formulated, a tendency can be seen in which social relations, which used to be based on trust and the assumption of innocence, are replaced by relations based on institutionalised distrust. If an increasingly comprehensive technology supports that development and if it seemingly dictates the – mostly provisional – boundaries, it affects the essence of the position of the individual in modern society.

Within the aforementioned social climate there is the risk of a reduction, if not erosion of the sense of the necessity to protect personal data. However, the protection of personal data serves underlying values. In addition to privacy protection

these values include the prevention of injustice and damage, equal treatment and prevention of discrimination, individual autonomy within certain boundaries and informational equality.

These values are not of a continuous equal order. Some serve a direct individual interest. Other underlying values such as trust, equality, freedom of communication or protection of physical integrity continue to be of high importance within the current social climate for a free and democratic society which our society is and wishes to continue to be.

In 2005, the Dutch DPA invested in the reconsideration of the objective of the WBP, the underlying values when protecting personal data and the manner in which these objectives and values can be best served by the supervising authority. Such a reflection cannot be conducted sensibly within splendid isolation. In 2005, the Dutch DPA, much to its delight, deliberately and regularly sought to exchange views and debated with experts and social parties, sometimes in a more contemplative context and sometimes in a direct relation to the necessity as the supervising authority to choose a viewpoint in respect of social developments. The Dutch DPA shall continue to do so.

The formal evaluation of the WBP is scheduled to take place in 2006. This evaluation is without a doubt useful. All sorts of considerations shall ultimately determine the practical implementation of this evaluation. The Dutch DPA, within the context of the evaluation, first wants to consider what values are at issue. In addition, the current question arises whether the WBP has contributed or could contribute to the protection or further expansion of those values. And only then the question whether the contents and formulation of the Act and the powers and responsibilities stipulated therein need amending, with a view to the social tendencies outlined above, becomes important. The WBP is a tool. The essential dilemma is the need for both control and trust.

Jacob Kohnstamm
chairman