

FOREWORD

This Report to Parliament is substantially based on the results of the Rathenau Institute's Privacy Project that ran from September 1996 to March 1998. The focal point of the project was the concept of privacy. Special attention was therefore paid to the Personal Data Protection Act (PDPA). The results of the project have been published in Privacy geregistreerd (Privacy registered), a collection of eight essays on privacy, and Privacy Vrijheid! (Privacy/Freedom) by Professor N. S. Gutwirth. The project was guided by a committee chaired by Professor A.W. Koers, Member of the Board of the Rathenau Institute. Project coordination was in the hands of drs. G. van der Starre and drs. M. Schoenmacker. This Report to Parliament is on the consequences of the use of personal data and the effect the PDPA has on it.

In the Rathenau Institute's Privacy Project, among other issues, attention has been paid to the increasing use of personal data. The project's conclusion is that it would be extremely difficult, if not unrealistic, to formulate a general normative framework within which the use of personal data can be regulated. However, two important effects of the use of personal data have come to the fore in the project: information stalking and risk selection. These two subjects are discussed in this Report to Parliament, together with the effects the PDPA will have on them.

Increasing use of personal data

Personal data plays a role in an increasing number of economic activities. Not only does it have a supporting place in business and industry, personal data as such also has an economic value. These developments are greatly facilitated by information and communication technology (ICT). By coupling databases, it has long been possible to retrieve information, store it, make connections with it, match it and process it. This can be done increasingly faster and more effectively by making

use of new techniques such as data mining¹ and data warehousing². With the availability of reference indexes such as bank account numbers, e-mail addresses and social security numbers, there is now the ability to generate new information from personal data. If data is sufficiently current, reliable and complete, it is then comparatively simple to obtain a detailed picture of the activities, financial transactions, preferences and habits of a person or groups of people.

This ability is of great advantage to practically every organization, especially in terms of marketing and business activities. Business sees it as a necessity to make optimal use of the possibilities provided by this advantage. For, because of further penetrating market mechanisms, the saturation of consumer markets, and increasingly fiercer competition, businesses can often only grow by continually using more sophisticated marketing methods. Getting to know the client better is therefore a priority, and the client profile can then be used to obviate, for example, financial risks.

Government also explores and uses the possibilities provided by the new techniques to render better service, for purposes of supervision, the maintenance of law and order, and for purposes of investigation. By connecting databases and matching data on incomes, forms of cohabitation, and property, the public can become aware of rights which they, as yet, do not claim, as the Municipality of Groningen has suggested in connection with rent rebate. Further, incidences of fraud can be detected in this way. With this purpose in view, the

¹ The search for relations and patterns in large data bases, without defining any possible relations beforehand.

² Establishing a collection of operational databases in which information is stored which can be used to support a decision process.



data exchange - based on statutory regulations - between (semi-) government bodies is increasing. In the mean time, also the internal functioning of the authorities is to a great degree dependent on automated systems, with personal data as an important source of information.

Two consequences of the use of personal data

Current practice in the processing of personal data exhibits two developments that demand a political evaluation in the light of the Personal Data Protection Act. We differentiate between the developments under two headings: 'information stalking' and 'the consequences of risk selection'.

Information stalking

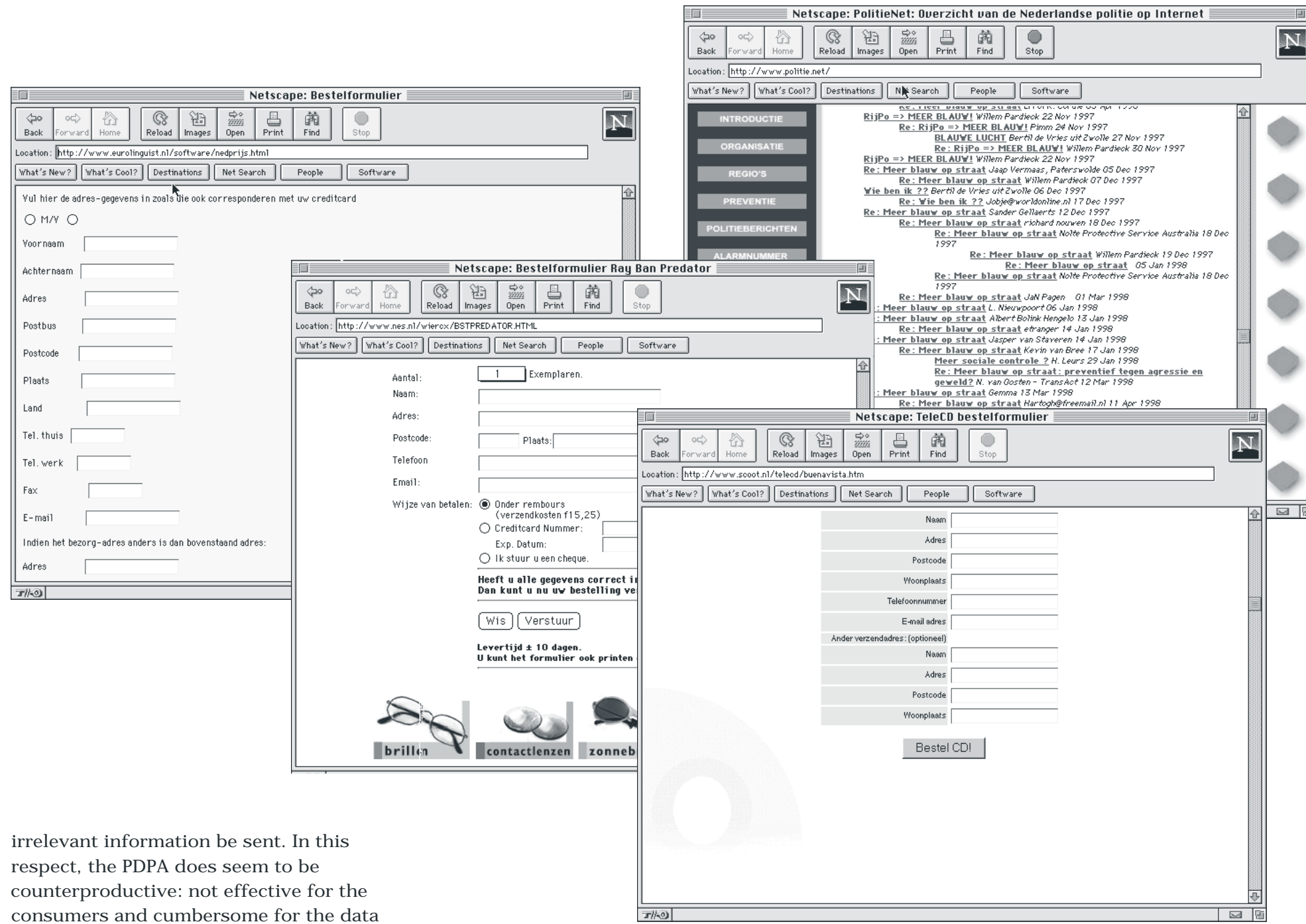
Organizations, both profit and non-profit, wish to sell products, gain support

for a good cause, conduct surveys for research purposes, and inform people of special offers etc. They use new marketing techniques to achieve these ends. The organizations derive their information on people from available databanks; there are currently thousands to be found on the Internet. Sometimes they pay for the data, sometimes they build the databanks themselves by, for instance, making use of customers' chip-card data to keep abreast of the products customers buy in the supermarket. This data is used to select and approach target groups. The practice can lead to piles of advertising material in the mail box, ever-increasing numbers of telephone calls from telemarketing firms, overflowing e-mail mailboxes, and software that is transferred to the hard disk without being perceived (cookies). This unsolicited bothering of people with information can be called 'information stalking'. It is a source of irritation for

some. It costs time, means waste of paper, and is experienced as a bothersome interruption of other activities. Others, conversely, do not find these things a problem because they think they are to their advantage. They merely ask themselves with some astonishment "How did they get my particulars?" Or, "How did they manage that?" Still others give a shrug, as long as it suits them, and then only in connection with things they are interested in.

What effect on information stalking can be expected from the PDPA? The PDPA imposes a number of restrictions on the users of personal data, such as limitations on the purpose to which it is put (data is to be used only for the purpose for which it is gathered) and transparency of processing. This should ensure that consumers are able to determine the purpose for which their data can or cannot be used, and that they would have to give permission for its processing. Bearing in mind current practice, where personal data is continually being processed, consumers would constantly, and on a massive scale, have to give permission for its use. The question is whether this is possible or even realistic. The practical possibilities of tracing infringements, let alone addressing them, is also in question, given, in practice, the extent to which data is processed. In addition, it can be noted that it is in the very interests of the processors to use personal data in a way that prevents information stalking as much as possible. It is precisely to establish who does not belong to the target group that personal data is necessary.

In brief, if processors conform to the rules of the PDPA, individuals stand the chance of being constantly approached for permission to use their data. First irritated by the folders, now individuals are continually being bothered for permission to match their postal code and personal interests so that no



irrelevant information be sent. In this respect, the PDPA does seem to be counterproductive: not effective for the consumers and cumbersome for the data processors.

Risk selection

Employers, credit providers, insurers and many others can, by using personal data, easily identify and select individuals. The technological possibilities have created in many organizations, businesses and institutions what can be called a 'hunger for data'. By this is meant the possibility, by the use of personal data, to anticipate risks and to locate risk groups. If these risks are found to be too great, exclusion from work, financial services and insurance can be the consequence. This situation can have far-reaching effects.

Someone who is not eligible for a life insurance policy will also have difficulty in obtaining a mortgage on a house. Employers will attempt to obviate the risk associated with a sick employee now that the costs associated with sick employees have to be borne to an increasing extent by the employer. The lives of individuals can be severely damaged if it should prove that the use of personal data leads to exclusion from or non-eligibility for a particular provision or service.

On the one hand, in terms of efficient management, this development is understandable. On the other, it gives rise to questions to do with the principles of equal treatment and the division of resources, in particular in respect to the far-reaching privatization of collective facilities. Where once these were the responsibility of public authorities, they are increasingly being operated by private organizations. Think, for instance, of the implementation of regulations in the social security arena. The changes there are accompanied by

the shift of an enormous bounty of personal data into the hands of commercial services.

What effect can the PDPA be expected to have? In any case, the PDPA will make things more difficult for the various organizations. It will become, both for marketers and risk evaluators, more laborious to acquire their relevant information (though for some sectors exceptions have been made). The question is whether the problem of exclusion has thus been ameliorated. It can be expected that businesses and other organizations, to keep their heads above water in a steadily more competitive economy, will continually seek means to exclude risks. The discussion must therefore extend beyond the handling of personal data only. Exclusion in itself is to be put on the agenda as a point of discussion. The Equal Rights Act already makes some provision for this, but the issue is the extent to which something like a safety net is to be created for people who, financially, might fall by the wayside.

The PDPA provides no protection against the consequences of risk selection. Therefore, what is or is not acceptable in the context of the society as a whole must be more narrowly examined, for instance per sector. And, on this basis, agreements must be come to, legally embedded or not.

Privacy

Information stalking and risk selection are, in the view of the Rathenau Institute, the two primary effects that must be examined in connection with personal data processing. Discussion on the regulation of the use of personal data often goes hand in hand with the discussion on privacy. In its Privacy Project, the Rathenau Institute examined the connection between the use of personal data and (invasion of) privacy. The conclusion reached by the project is that it is certainly no sinecure to

establish this connection. There is no consensus as to the definition of the concept of 'privacy'. The definition of privacy and the importance of privacy differ from individual to individual and from situation to situation. Wide differences also exist in the perception of privacy, from generation to generation and from culture to culture. The perception of privacy at the start of the seventies was not the same as it is at the end of the nineties. Nevertheless, the PDPA appears to proceed from the perception that there is a strong need, felt by everyone, to protect personal privacy. This is expressed in the restrictions placed on the processing of personal data.

In spite of the lack of consensus on the definition of privacy, it is still important to pay attention to the, often deeply held, conviction of some people that the unrestrained processing of personal data could lead to a world where everybody can learn everything about everybody else, to an 'Orwellian' society. In such a world situations could arise in which, for instance: personal data can be used in all "the capillaries of the government body"; it will be extraordinarily difficult to protect yourself against powerful Big Brothers; you'll be stigmatized life-long by what the system knows about you; you will never again be able to present yourself in a different light, and all the decisions made about you will be based on what the system has to say about you. While the predictions made in 1984 have never come to pass, the means by which people can maintain their faith that such a scenario will never come about must be looked into. Here is a task for the Data Protection Authority. In this connection, the Rathenau Institute deems it vital that the Data Protection Authority clearly defines what is meant when it signals an 'invasion of privacy'.

Conclusion

Government has with the Personal Data Protection Act chosen a means of



implementing the European guidelines on the processing of personal data that does not address two important consequences of data processing: information stalking and risk selection. The Rathenau Institute realizes that the Netherlands government is obligated to implement the European guideline on the processing of personal data. This, however, does not have to be as far-reaching as the legislature now has in mind in respect to the PDPA. It appears more desirable for the present to restrict the PDPA to the content of the guideline and to define a trajectory that will enable keeping up with current and future developments in respect to personal data. This would enable the implementation of measures more appropriate to the current situation and to future situations. Not only the processing of personal data, but, in particular, the effects of the processing

must be the subject of research and monitoring. ICT developments, after all, are moving rapidly. Innovation continues to play a major and significant role and organizations continue to look for new challenges in ICT. The role personal data will play in all this remains a constant issue. Under the pressure of both technological and economic developments, border-lines keep shifting, not only in respect to what is possible but also in respect to what is found to be acceptable and decent within the society as a whole.

The Data Protection Authority has been allotted an important task in the PDPA. The Rathenau Institute pleads that the Data Protection Authority ensures that the consequences of personal data processing practices be subject to constant monitoring and research.

Report to Parliament is a publication of the Rathenau Institute.

The Rathenau Institute is an independent organization whose task it is to support social and political opinion-forming on issues having to do with scientific and technological developments.

The Rathenau Institute provides the Dutch parliament with the results of its projects.

First published in August 1998.

Original title: Bericht aan het parlement over persoonsgegevens in de informatiemaatschappij.

Text:
Margot Schoenmacker and Gijs van der Starre

Translation:
J.B. Zaat-Jones, English Only, Oegstgeest

Photography:
Hollandse Hoogte, Amsterdam

Report to Parliament is printed on
100% recycled paper

Design: Basislijn, Amsterdam

Editorial address:
P.O. Box 85525
2508 CE The Hague

Telephone: + 31 (0)70 - 3421542
Fax: + 31 (0)70 - 363 34 88
E-mail: Rathenau.instituut.@rathenau.knaw.nl
Internet site: <http://www.rathenau.knaw.nl>



Background photograph: Bart Versteeg

In passing the Personal Data Protection Act (PDPA), the Netherlands fulfills its obligation to implement the European guideline on the use of personal data. Two important societal consequences of the use of personal data are 'information stalking' and the increasing possibility of risk-selection. The PDPA is not intended to protect against these effects. That will require other measures.

Personal data in the information society

This Report to Parliament is linked to the discussion on the implementation of the European guideline, "in the matter of the protection of natural persons in connection with the use of personal data and in the matter of the free traffic of that data". The implementation is to be concluded in the Personal Data Protection Act (PDPA)

which replaces the Data Protection Act (DPA). The most important purpose of the guideline is to guarantee the free traffic of personal data within the European Union by eliminating the differences between the member states in connection with the level of protection of personal data.