De Wet persoonsregistraties

norm, toepassing en evaluatie

Proefschrift

ter verkrijging van de graad van doctor aan de Katholieke Universiteit Brabant, op gezag van de rector magnificus, prof. dr. L.F.W. de Klerk, in het openbaar te verdedigen ten overstaan van een door het college van dekanen aangewezen commissie in de aula van de Universiteit op vrijdag 8 september 1995 om 14:15 uur

door

Margriet Overkleeft-Verburg

Promotor: prof. dr E.M.H. Hirsch Ballin

Inhoudsopgave

Summary

1. Introduction

This study is the reflection of research into the functioning and effectiveness of the Dutch Data Protection Act (Wet persoonsregistraties, WPR). It is intended as a study for the new privacy legislation that is needed to implement the EC Directive for the protection of personal data. The emphasis lies on the structural components of the WPR, in particular on experiences with concepts in the law and the functioning of the system of self-regulation at sectoral and operational level. This evaluation results in a number of concrete recommendations for the new Dutch privacy act, that will replace the current act by January 1st 1999.

2. History of WPR development

The right of privacy traditionally is strongly integrated in the Dutch system of law, in the Constitution, written and unwritten secrecy pledges, specific laws and judicial decisions; it is sanctioned by criminal law, civil law and disciplinary rules. From the viewpoint of norms, the system has been rather effective and also very flexible, although fragmented with a heavy emphasis on casuistry. The debate on threats against privacy started in the 1960's, initiated by the emergence of computerized information processing. The immediate causes were the plans for modernization of the municipal registry office, culminating in proposals for an automated central population registry and the implementation of a general registration number. Apart from the desire for more efficient government administration, the proposals were linked with the necessity to extend government information provision because of the expansion of the welfare state (planning, execution and evaluation). The objections culminated in a widespread civil protest against the census of 1971. The number of persons refusing to cooperate was such that the census was deemed a failure. It was never attempted again.

In response to this, the government had decided, already in 1971, to develop general privacy legislation addressing the registration of personal data. At that time also, while revising the Constitution it was decided to incorporate in it a general right on privacy, apart from the inviolability of the home and confidentiality of personal communications. In 1972 a state committee was charged with the preparation of the privacy law. This committee published its findings in 1976, together with the draft regulation. These proposals, based on the then current state of the art in mainframe information processing, opted for a system of individual regulation of personal data files, in combination with a precursory review on legitimacy by the Registration Chamber. On the basis of these proposals, a bill was put forward in Parliament in 1981. The proposal was much criticized, especially with regard to the potential problems of implementation, caused by the rapid growth of automated data processing and the emergence of the personal computer. Because of this the bill was withdrawn, and in 1985 a new one with a different system of regulation was put forward. This bill was accepted in Parliament and enacted on July 1st 1989 as the Wet persoonsregistraties (WPR). The main implementing order, the Sensitive Data Decree, was only enacted on May 1st 1993. Internationally, the Netherlands had become a laggard, as opposed to holding its former frontrunner role. The reason for this delay in the legislation process was the necessity to replace the system of precursory review proposed by the state committee with another system based more on repressive supervision and the priority of the Data Protection Bill relative to other legislative projects.

The fact that specific privacy legislation failed to appear, didn't greatly hinder the further development of privacy protection law. In interaction with the discussion on proposals for a new data protection act, regulation occurred along three lines. By the privacy directive of the prime minister of 1975, the obligation was put into effect to have a privacy charter for each automated personal data file within the (central) Dutch government. By means of local privacy regulations, this same obligation was implemented by many local authorities. This form of self-regulation was also used by some of the private sector. Apart from this there also emerged more sector-specific regulation of information processing. By a dynamic interpretation of existing rules, in particular based on the law of torts, the Constitution and the Freedom of Information Act, the judiciary

contributed strongly to the formation of new law. The emphasis therein lies largely on a balance of interests, where the privacy element and the legal position of the data subject are explicitly taken into account. This development made the WPR, when it came into force in 1989, largely a codification of existing privacy practice. The history of development of the WPR is however still of rel evance because of the effect of dated concepts. An important number of the obstacles identified in this research find their source in this history.

As a consequence of this development, the complexity of privacy law in the Netherlands is substantial. The WPR has only partly obtained its intended central place in legal practice. Moreover, this research shows that the judge, being much acquainted with balancing interests on the basis of current private and administrative law, is often inclined towards a rather restrictive interpretation of the WPR. Because of this privacy law is now a combina tion of general privacy legislation, regulation of privacy aspects in other law, constitutional rights and case law. The complexity created by this situation is further aggravated because the WPR is in its own way a driver of sectoral law. Recent years have brought about new legislation on the automated population register of the local authorities and specific regulation in fiscal law, social security regulations and legislation on personal identification, all aimed at increasing the efficiency of information processing by the authorities and aiding in the fight against tax fraud, misuse of social securities and such. In view of this, the impact of the WPR alone on information processing by the authorities should not be overestimated.

3. Structure of the WPR

The WPR is a product of the obligation, incorporated in the Constitution since 1983, for the legislator to provide regulation. This act also implements the European Convention for the Protection of Individuals with regard to Automated Processing of Personal Data of 1981 and the obligation to regulate that is contained in article 8 ECHR. This act is structured as a system of tiered norms. In the act, a regulation of the legal position of the data subject and the functions and competencies of the Registration Chamber are combined with direct clauses governing the creation of a personal data file, the filing of personal data, the legitimate use of filed personal data and the issue of said data to third parties. These norms are differentiated on the basis of a distinction between the public and the private sector. The act provides for a further differentiation of these global norms in two stages. The controller of the file is obliged to give notification and to provide for self-regulation with regard to each individual personal data file. There is an exemption from these obligations for certain categories of personal data files that meet requirements stated in the Decree on Conditional Exemption and that follow the standard rules mentioned therein. Apart from this, the act provides for self-regulation at the sectoral level in the form of a code of conduct that is specific for the information processing in that sector. The code can optionally be submitted to the Registration Chamber for approval. This code of conduct is an inter mediate construct between the regulations in the act and self-regulation at the operational level. The act provides for the competence to decree supplementary regulations at the sector level.

4. Experiences with the system of self-regulation by sector

In mid-1995 16 codes of conduct, based on the WPR, are realized at the sectoral level. More than half (9) are approved by the Registration Chamber. For six codes, the procedure is still ongoing. The stimulus towards self-regulation that the legislator gave, has had its effect. No use was made of the power to decree regulation at the sectoral level, as opposed to self-regulation.

As intended by the legislator, the codes of conduct are mainly used in the private sector, in particular in the professional services segment (direct marketing, market survey, trade information, data processing, recruitment services) and in information-intensive branches (mail orders, pharmaceutical industry, publishers of periodicals, employment agencies, banks and insurance companies). Furthermore, codes of conduct have been realized for the social research sector and health research. No codes of conduct have been realized in the public sector.

The normative significance of the codes of conduct is diverse. The emphasis is on specialization of clauses in the law on specific use of information processing in the sector. Also, some codes contain complementary clauses. In several cases the code of conduct has been based upon existing privacy norms and/or professional codes or codes of ethics. Not all the results obtained by the codes of conduct are therefore attributable to the WPR. In part, the codes are a new formulation of existing regulation. It has been shown that the margins for self-regulation are dictated by: (a) the generic nature of sectoral regulation, (b) the completeness of regulation in the WPR, (c) the standard regulation offered by the Decree on Conditional Exemption, and (d) in some cases the absence of a unified pattern of information processing in a sector. In setting up a code of conduct, there is a preference to realize a complete regulation of the information processing. This is the reason why many codes contain a fair amount of "parrot clauses" that copy those in the WPR. It is of interest that codes of conduct up till now have not been used to regulate new products and services. On the whole, the codes of conduct do however have a substantial contribution to the protection of the privacy of data subjects. This protection consists mainly of an increase in legal security and transparency of the information processing by means of specialization of norms and standards in the sector and by the incorporation of additional provisions like procedures to handle complaints and disputes. This form of regulation still has a potential for growth. However, it needs continuous maintenance in the form of confirmation, enforcement and actualization of the norms.

This research shows that the functioning of self-regulation at the sectoral level meets the intention of the legislator to a large extent. By means of the code of conduct and focused support of their members, the relevant branch, sector and professional organizations have shown that they feel themselves responsible for the implementation of the WPR in their sector. The social basis of the act has been broadened by the codes; they have also speeded up the process of implementation. The possibility of a preventive review by the Registration Chamber has been beneficial with regard to legal security both for the controller of the data file and for the data subject.

The code of conduct has also shown itself as a way of regulation with inherent constraints and risks. These mainly stem from the tension and the potential conflicts between the law as enforced order (top down) and the discretionary nature of self-regulation (bottom up). This tension manifests itself mainly in the consumer sector. The question arises whether the privacy regulation is a consumer matter and as such the full responsibility of the parties in the market, or whether it is part of an interlinked set of regulations controlled by the government. The codes of conduct have had some unexpected side effects. Most striking of these is the susceptibility to conflict of the procedure of approval by the Registration Chamber. This is mainly caused by: (a) the lack of consensus on the starting points of the WPR, (b) the existing ambiguity in concepts of the act, (c) the effect of interpretation of the act on the level of implementation costs, (d) the expectations about the margins for regulation of the sector organizations, and (e) diverging opinions about the functions and the competence of the Registration Chamber. What was lacking in the WPR was made manifest by the procedure of approval. This is more a process of negotiation between the sector organization and the Registration Chamber, which had to compensate for the defects in the legislation process by means of the codes of conduct. In this respect there was a form of extended legislation because some relevant issues were passed on from the legislation process to the implementation process. An additional problem was the lack of any possibility of appeal in court to resolve an impasse.

Further unintended side effects of the self-regulation at the sectoral level are: (a) supplanting the act by self-regulation, (b) use of self-regulation as a way to oppose and counteract the functioning of the WPR, and (c) the possible confusion of parties concerned by the fact that some codes of conduct are approved by the Registration Chamber, while others are not. Obstacles in the approval procedure, apart from the lack of any possibility for appeal, mainly concern the obligatory participation of relevant interest groups in the process of specifying a code of conduct, the lack of any formal rules for the procedure, and in particular the lack of any time limits on the decision process of the Registration Chamber.

A further characteristic of self-regulation in this context is that it requires constant attention and reinforcement, in particular in the relation between the sectoral organization and the Registration Chamber. If this attention is lacking, the normative value of the code of conduct will deteriorate. Evaluation of this regulation tool is therefore only a picture at a given moment in time; success in the long run will depend on the continuous efforts of all parties concerned, the Registration Chamber included.

5. Function of the Decree on Conditional Exemption

The WPR provides for a system of tiered norms, resulting in a set of specific operational instructions for different types of information systems. For certain categories of personal data files standard regulations are specified in the Decree on Conditional Exemption (Besluit genormeerde vrijstelling, BGV). This decree mentions 19 standard specialized regulations for membership data, subscription data, personnel and payroll systems, financial administrations, customer files, registry of pupils and students, permit / licence administration and archives. Whenever a personal data file falls within these categories, the standard norms apply and exemption from notification is implicitly given. If the standard norms are not applicable or the controller decides, for other reasons, to specify different norms, the controller has to provide for self-regulation. The personal data file should in this case be registered by the Registration Chamber. The legislator intended that the following objectives be realized by the Decree on Conditional Exemption: (a) to differentiate between personal data files with a stronger or lesser degree of sensitivity of the stored data, (b) standardization of norms at the operational level, and (c) deregulation and reduction of the cost of operation.

The norms of the decree are more strict than those of the WPR. The decree is based on a traditional typology of information systems dedicated to a single function and is in part very detailed. Because of this the decree cannot, without some very artificial reasoning, be applied to information systems that service multiple functions. Although it was not intended that way, the decree increases the complexity of the legislation by a combination of legal norms in the WPR, operational instructions in the decree, the effect of specific legislation and supplementary regulation by the controller of the file. The need for advice and interpretation remains high, as does sensitivity to conflict. Furthermore, the decree has proved to be ineffective as far as differentiation and reduction of operational costs are concerned. There are clear signals from the field that the decree is seen as a collective exemption from the obligation of notification, and not, or insufficiently so, as a set of compulsory norms. The indicated problems are of a structural nature, as they are strongly related to limits of the legislator's power of regulation. It is stated that this kind of a detailed, cross-sector and type-dependent general regulation of personal data files is no longer a viable option.

6. Function of the obligation of notification and self-regulation

In order to gain a clear view of the observance by individual controllers of the obligation of notification and self-regulation, a quantitative analysis was made of the personal data files held by the Registration Chamber as at January 1st 1995. From January 1st 1990 up to January 1st 1995 more than 50,000 personal data files were registered, 35,000 by some 15,700 controllers from the public sector and 15,000 by 12,700 controllers in the private sector. Of the 15,700 controllers in the public sector, some 11,900 belonged to the category of (para)medical professionals. Of the 35,000 data files in the public sector, a total of 16,000 came from health care, and 12,900 were in the care of local authorities. Local authorities and hospitals were also chief amongst those controllers with a big number of registered data files, with a maximum of 223 for a single hospital and one local authority giving notification of 224. The number of controllers in the private sector (12,700) is less than 2% of the number of organizations entered in the Dutch Trade Register. Moreover, there is a clear imbalance caused by an overrepresentation of some sectors, notably those where the branch or sector organization has been active in supporting their member in the notification and self-regulation process. The maximum number of data files from a single

controller (17) is far less than in the public sector. Many firms clustered their notification at the holding level (banks and insurance companies).

Notifications in the private sector were dominated by customer files (85%) and personnel administrations (9%). The majority of data files in the public sector also belong to these two categories. A significant part of the notifications concerns data files that are (fully or in part) kept manually. Personal data files registered by the Registration Chamber differ widely from simple straightforward files for a single purpose to complicated, multifunctional information systems containing (in part) very sensitive data.

The curve of notification shows that observance of the obligation of notification was concentrated in the first phase of the implementation of the WPR, the period from January 1st 1990 to July 1st 1991. Since then the volume of notifications in the private sector has been on a rather low level. The decline of the notification volume from the public sector has been more gradual, and ever since early 1993 this volume also has been rather low. The number of changes to the data kept in the register of the Registration Chamber has been lower than might have been expected, although the WPR prescribes that notification be given whenever a change occurs that affects the data in the original notification. Apart from the fact that the data in the register are thereby becoming out of date, this also means a decline in the effectiveness of self-regulation on the operational level.

A random sample from the register has shown that the quality of notification and self-regulation differs widely. A substantial percentage of the received notifications and regulations is not up to standard. Many of the controllers seem to have perceived it as a one-time obligation of a purely administrative nature. In general, it seems that self-regu lation has functioned best were it could build upon a tradition of secrecy pledges and careful treatment of personal data, or where the privacy regulations also functioned as internal instructions or procedures or could be of value as a marketing tool. The obligation of self-regulation was in those cases the starting point for an exercise that was also of benefit to the organization itself. Although showing some positive results, the findings on the observance of the obligation of notification and self-regulation are largely disappointing. It is ignored by many, or only taken as a token obligation. Even an active enforcement policy by the Registration Chamber cannot be expected to change this radically.

The obligation of self-regulation consists of choices from options that are legitimate as such, while further constraining the normative latitude that the WPR provides for the controller of the file. One should therefore make an explicit distinction between the obligation of notification and that of self-regulation. Apart from this normative aspect of self-regulation, consisting of a self-imposed restriction within the margins of the law, the obligation of notification and self-regulation also provides for information and internalization functions. The information function provides transparency and controllability of information processing for the data subject, other parties concerned and the Registration Chamber. The internalization function concerns the obligation of the controller to explicitly balance the interests of all parties concerned, which will increase the awareness of privacy issues. The obligation of notification has only an information function, in contrast to that of self-regulation, which functions primarily as a basis for a more restrictive regulation than the law provides. This obligation of self-regulation is a carry-over from the proposals of the state committee of 1976. The binding nature of the description of the information system remains, while the preventive check has been replaced by a system of repressive surveillance.

Such a system of self-regulation at the operational level can be effective, provided that the following conditions are met: (a) the information system subject to regulation is sufficiently stable over time, (b) there has been an adequate survey of existing and foreseeable information needs, both structural and incidental, (c) the effects of the law on concrete information relations can be precisely defined (d) the legal regulations exhibit a sufficient degree of flexibility, and (e) the controller is willing and able to define and impose his own regulations. Because these conditions are not always met, the functioning of the obligation of self-regulation in the WPR has revealed many problems. Apart from the operational problems that are caused by the act itself, mainly due to inadequate definition of concepts, unclear definition of the scope of the law, imperfect

demarcation in sectors and insufficient clarity in the interaction between legal norms and self-regulation, the applicability of adequate and concrete operational instructions is constrained by parallel formation of law, that carries over into the application of the WPR. The above is especially true for: (a) the impact of legislation on freedom of public information, (b) case law on the basis of the civil code as a source of (unwritten) information duties, (c) the effect of written and unwritten secrecy pledges, and (d) the increase, initiated by the WPR, of registration and information duties in sector-specific laws. Part of the relevant norms cannot be made concrete because of the obligation to balance interests in the context of the actual situation. The legal complexity of the obligation of self-regulation has therefore been underestimated. Neither was there, at the time of the introduction of this obligation, sufficient thought for the inherent tension and susceptibility to conflict that exists between the conservative aspects of self-regulation and the orientation towards flexibility of multifunctional information systems. In this context the capability for regulation by the controllers, the identifiability and predictability of information needs, have been estimated in a much too optimistic way. Also, the contraproductive side effects of such a system of regulation have been underestimated, especially those that stem from bureaucracy and a fixation on formalities. Because of this the real legal issues tend to be pushed aside. Moreover, the emphasis on privacy aspects in the relation between the controller and the data subject presents the risk that third-party and public interest could be threatened. A balance of interests cannot be guaranteed in this system.

Because of the shortcomings indicated in the normative function of self-regulation at the operational level, the information function, aimed at transparency and controllability of information processing, also has not been fully realized. The results of the internalization function, aimed at increasing awareness of privacy issues and norms, have been diverse. Enactment of the WPR has, unmistakenly, contributed to activation and a focusing of awareness that was partly already there. This activation was clearly noticeable during the first phase of the implementation. At a later stage the effect gradually diminished, and observance of the obligation of self-regulation became a (one-time) administrative chore.

Based on the foregoing, the conclusion has been made that the obligation of notification and self-regulation at the operational level has not been as effective as intended. This lack could not be fully compensated by the efforts of sector organizations at their level. As such the ambition of the legislator has proved to be insufficiently realistic.

7. Function of the WPR's structural components

Legal position of the data subject

Some of the objectives of the legislator have been realized quite well. This is especially valid for the enforcement of the legal position of the data subject, in particular his rights with regard to information, access and rectification. Although these rights had already been endorsed by the judiciary as elements of the basic right to privacy, the WPR has substantially added to this legal security, particularly where information from manually maintained files is concerned. The legal right of information, access and rectification is being used selectively, focused on the direct relevance of the data file to the data subject. The greater the consequences of registration for the data subject, the more use is made of the right of information, access and rectification. This shows in the steady increase in information requests addressed to the BKR (Bureau Kredietregistratie), the organisation that maintains the database where certain debts of private persons to financial institutions are registered. In 1988 there were 8,500 requests; in 1994 this number had increased to 19,000, and it is still climbing. When there is no directly recognizable consequence of being registered, the number of information requests is far lower. This selective use of the rights incorporated in the act can also be illustrated by the use of the Mail &Telephone Preference Service, the central registration by the direct marketing sector of persons who do not want to receive direct mail or calls from telemarketing agencies. The size of this file remains steady at about 75,000 registered addresses, even though registration is only valid for a period of five years.

Involvement of the sector organizations

A second positive experience is the willingness of the sector, professional and umbrella organizations to participate in and take responsibility for an adequate level of privacy protection. Apart from the results in self-regulation at the sectoral level in the form of codes of conduct, as described above, this commitment has manifested itself in the specification of model regulations, the information services and the active support of their member organizations in observance of the obligation of self-regulation at the operational level, and their intermediary and representative role in contacts with the Registration Chamber. In this context public opinion (consumer trust) has proved a very effective countervailing power. In the consumer sector especially there is a continuous and intensive interaction between innovation and public acceptance. As a factor of real commercial relevance, public opinion proves to be strong in setting the boundaries, perhaps even stronger than the legal norms. Codes of conduct that have been realized also show this effect. The choice in the WPR for primacy of self-regulation at the sectoral level has proved to be correct.

Obstacles in the WPR, the definition of concepts

A number of obstacles were indicated that found their origin in the WPR itself. The partly deficient and dated definition of concepts in the act are a source of implementation problems. This is especially valid for the concepts of "controller," "personal data file" and "personal data".

The concept of controller

During the debate in Parliament, the concept of controller was given a hybrid meaning. The controller could be a natural person, a legal entity or a competent governing body, but also a functionary or civil servant to whom this responsibility has been delegated. Responsibility for the operations was put on a line with authority over information processing. This is contrary to current private and administrative law concerning persons and organizations. The Registration Chamber has tried, through public relations and approval policy, to promote the interpretation that a controller can only be a natural person, a legal entity or a governing body. The Chamber has only partly succeeded in this. The public sector in particular continues to appoint civil servants as controller. In education, health care and social services, it is the director of the organization who is the controller in most cases. Such an interpretation of the controller concept is a potential source of problems as it does not fit with the existing hierarchical relations and the competence to define what tasks are done and how they are done. Although the controller function in the private sector has not been delegated to a subordinate level, filling in this function was, also there, not without problems, mainly because, during definition of the bill, it was suggested that there would be a certain degree of freedom in shaping the controller function. The operational burden of the obligation of notification and self-regulation, combined with the wish define things in such a way that qualification of information exchange as third-party issue is kept to a minimum, led to a practice where, in certain sectors, the controller was defined at the holding level. On this issue an impasse exists between the Registration Chamber and the banks and insurance companies that cannot be resolved because of the absence of any possibility of a judicial intervention.

The concept of personal data file

The scope of the WPR is directly related to the interpretation of the concept of personal data file. The personal data file is also the object of self-regulation. The act concerns automated and manual personal data files that are systematically ordered. In practice this concept causes some confusion. As far as the automated data files are concerned, there are problems as to what should be designated as such. This is especially valid for multifunctional information systems. The question arises whether the actual structure of the information system should be taken as a starting point or whether a multifunctional information system should be considered as several separate systems, each with its own support function. The Registration Chamber nowadays is inclined to the second interpretation. Most of the problems, however, arise from the question of which manually maintained files should be governed by the act and which not. The real question is what the notion of "systematically ordered" entails. The judge and the Registration Chamber

each interpret this in a different manner. In case law one can find both a limited interpretation of the concept of personal data file, in particular by the Hoge Raad and the Afdeling bestuursrechtspraak of the Raad van State, as well as an interpretation by a section of the lower judges that intends to maximize protection by law. The Registration Chamber has made a policy switch with regard to the issue of systematic ordering of manual data files. The Chamber now considers nearly all manual files that are routinely maintained in organizations, to fall within the scope of the WPR. The real issue is the usability of the data files, with the ability to locate individual files/dossiers as a minimum requirement for being systematically ordered. The availability of even a minimal index, e.g., a table relating a name to a file number, is deemed to be sufficient. The concept of personal data file is being widened. Of late the Registration Chamber has termed a file on commercially available CD-ROM as a personal data file, as well as a collection of wordprocessor documents that could be accessed by means of some selection criteria. The legal insecurity that is a consequence of the above creates risks, both for the controller and for the data subject.

The concept of personal data

Whether a data file can be identified as a personal data file in the terms of the WPR, is dependent on whether personal data are stored therein. Application of the criterion of "information that relates to an identified or identifiable person," has proved to be a matter of dispute, in particular with regard to information processing in support of social and medical research. According to the Registration Chamber, only those files containing data that cannot possibly be related to an identifiable person, even with the use of vast data processing facilities and extensive knowledge of the subject matter, will not be defined as personal data files. The research sector promotes a more moderate view, where contractual obligations and codes of conduct are taken into account when estimating the chance that information in the files will be related to identified persons. A second source of problems concerns the difference between information about a person and information about a company or organization. The Registration Chamber uses an extensive interpretation, causing a major part of the files supporting business-to-business relations to be defined as personal data files and thus be subject to the WPR. This is contrary to views and expectations in the private sector.

Complexity of regulation

The diversification of information regulations in sectoral law and the carry over in the WPR of (in part) unwritten secrecy pledges (professional secrecy in the medical sector), (international) basic law and obligations stemming from international treaties, have resulted in a very complex regulation of information processing. It cannot be guaranteed that new law is always tuned to existing law, in particular to the WPR as a central privacy regulation. This is not only valid for the material norms, but also for competencies in enforcement and for the nature of legal security. The above not only causes privacy norms to be liable to conflict and dispute, but also bars access to the subject matter. This has damaged the legitimacy of privacy norms. For this reason, there is an urgent need for harmonization and coordination of existing regulations.

Position of the Registration Chamber

The position and functions of the Registration Chamber are not made sufficiently clear. Opinions differ widely in this respect. Some argue that the Chamber should be a "public watchdog," the champion of the interests of the data subject. The Registration Chamber has indeed made a policy change towards a more activist approach, where the "public pillory" method was not shunned. Contrary to this is the opinion that the Chamber has primarily an administrative function, and its operational tasks are emphasized. In this context the Chamber is charged, apart from the special care of privacy protection, with responsibility for the enforcement of the WPR, in particular with an obligation to ensure a balanced application of the law. This is especially valid for: (a) the approval of codes of conduct, (b) counselling and arbitration in disputes, and (c) enforcement of observance of the WPR and related legislation. On the basis of the foregoing, the Chamber has been given far-reaching authority to conduct inquiries. This opinion leaves the activist approach to privacy protection to the realm of public interest groups (consumer

organizations, patients' rights movements, etc.), possibly supported by government funding or facilities. It is well established that the two opinions are not compatible. An activist nature of the Registration Chamber would harm credibility and effectiveness of its administrative function and also its role as an impartial, authoritative and expert counsellor / arbitrator.

Intervention by the judiciary

In practice it has been proved that the current act provides insufficient means of conflict resolution. There are not enough checks and balances. This is mainly caused by the clause in the WPR that explicitly excludes the possibility of appeal in administrative court against decisions of the Registration Chamber with regard to approval of codes of conduct and positions taken. Although it is possible to institute legal proceedings against the State because of wrongful acts, this entails so many risks, that it is not a viable option. The lack of legal security translates to a heightened process risk that bars many from taking their case to court, which in turn preserves the lack of legal security. Impasses like those over the interpretation of the concepts of the act and the autonomy of the Registration Chamber to set it's own policy for the approval of codes of conduct, thus remain unresolved. This inhibits further development of the law. Secondly, the WPR refers to the civil court when the legal position of the data subject is at stake. In practice this often concerns interpretation of administrative law. Case law shows however that the administrative court finds itself competent to handle cases concerning the WPR.

8. Main recommendations

Based on the findings of this research and taking into account the scope for policymaking that the draft EC Directive gives to the member states, the following recommendations are made:

The positive experiences with the codes of conduct towards continuation of this form of self-regulation at the sector level. The draft EC Directive leaves room for an optional procedure for the approval of codes of conduct such as is incorporated in the WPR. It is recommended that the requirements for admissibility be changed and the procedure restructured and formalized, in particular by defining time limits for the decision process of the Registration Chamber.

It is recommended to define more rigorously the concepts of "controller," he who is held responsible for the information processing, and to align the concept better with current private and administrative law about persons and organizations. The concepts of processing manager and network manager should be added, and a further differentiation of the concept of processor will be needed as new forms of professional service emerge.

The demarcation of the concepts of automated data processing and manually maintained files needs further attention in the new implementation bill. These concepts should be closely aligned with the actual structure of the information processing. In particular attention should be given to the position of temporary files, text-processing files and back-up facilities. Furthermore, it is recommended to extend the scope of the act to include manually maintained files in line with the current position of the Registration Chamber on this matter. The act should differentiate according to the type of data file as far as inspection of data, costs and storage times are concerned. It is recommended that a separate regulation be defined for the production and use of CD-ROM and similar new media.

The new legislation should give special attention to the definition of the concept of personal data. In particular, care should be taken to distinguish information on companies and organizations from personal data. The norm should be differentiated according to the nature of the stored information. The status of files for statistical research at professional research institutes should be further clarified.

As the obligation of self-regulation at the operational level has proved to be insufficiently executable and enforceable, it is recommended to drop this obligation and leave regulation at the operational level to the controller, who can impose additional rules by means of a privacy regulation. Privacy regulations can be expected to keep their important role at the operational level in situations where the specialization of standard norms is considered essential by the controller's organization. In this research the position is taken that the obligation of self-regulation at the operational level implies a further restriction of the freedom of the controller compared with that provided in the draft EC Directive, as this obliges controllers to make a binding choice from a number of options all of which are lawful. If the obligation of self-regulation at the operational level is to remain in force, a legal basis has to be found in the draft directive. Apart from art. 20, on the freedom of member states to implement a selective preventive review with regard to information systems of a very sensitive nature, this basis cannot be found. Also for this reason, the obligation of self-regulation at the operational level cannot be maintained. Optionally, the act could contain an explicit encouragement to the controller to specify a privacy regulation. It is further recommended that the selective precursory review in the Directive not be implemented in the national legislation, as there is no indication of the need for such a review. Any form of mandatory notification should be regarded with reticence. The emphasis should be on the information provided via the data protection official, as mentioned in the draft EC Directive.

Apart from the emphasis on a further and more concrete definition of norms, it is recommended that the dogmatic embedding of the new privacy act in current law receive special attention. A combination of general norms and sector-specific norms, with the option to include new elements as soon as the need arises, is preferred. Also, the mutual tuning of privacy legislation and freedom of information legislation needs to be considered as well as the interaction between privacy legislation and the civil code.

It is recommended that legal protection of the controllers, the data subjects and other parties concerned be extended, in particular in relation to the decisions made by the Registration Chamber as the approving and enforcing body. The starting point should be that the function of the Registration Chamber be subject to the administration of administrative law. Decisions of the Registration Chamber should be made public, in line with existing rules for similar institutions.

The principles set forward in the Convention for the Protection of Individuals with regard to Automatic Processing of Data of 1981 should be reconsidered in view of the changed information situation. The criteria put forward in the article 7 of the Draft EC Directive, are a good starting point for this discussion.

These recommendations stem from the basic notion that the credibility and effectiveness of privacy protection is fully dependent on sound, executable and enforceable legislation and a balanced application of the law.