Chapter 9
Conclusion – Essential elements of data protection legislation

Contents

1 INTRODUCTION

After analysing different foreign data protection laws and legal instruments in chapters 2 to 5, a set of core data protection principles is identified in chapter 6. In addition, certain general legal principles that should form the basis of any statutory data protection legislation in South Africa are proposed in chapter 7 after an analysis of the theoretical basis for data protection in South African private law. In chapter

8 the current position as regards data protection in South-Africa is analysed and measured against the principles identified in chapters 6 and 7. The conclusion is drawn that the common law cannot be developed fast and efficient enough by the courts to establish a new data protection regime. Also, although the current South African Acts can all be considered to be steps in the right direction, they are not complete solutions. Further legislation incorporating internationally accepted data protection principles is therefore necessary. The aim of this chapter is to briefly summarise the elements that should be incorporated in a data protection regime.[1]

2 SCOPE OF DATA PROTECTION LEGISLATION

2.1 General data protection legislation preferable to sectoral approach

A general data protection statute that is supplemented by area-specific legislation or codes of conduct is preferable to a purely sectoral approach. A sectoral approach such as the one that has been adopted in the USA results in different levels of protection in different areas of processing. It also results in lacunae and inconsistencies in the protection of the individual's privacy.[2] This leads to confusion on the part of individuals, who do not know whether or not they have rights[3] that are enforceable against data controllers.[4]

2.2 Automatic and manual processing

1 The general theoretical principles explained in ch 7 par 5 should of course also be reflected in any data protection legislation.

2 The result may be that individuals' video records are protected, but not their medical records; or that medical records are protected in the public sector, but not in the private sector. Gellman 2000 *Gov Inf Q* 235, 237 states with reference to the position in the USA: "The existing patchwork quilt of sectoral laws leaves many significant personal records with no privacy protection at all."

3 Eg a right to access their data or to correct inaccurate data.

4 See eg ch 2 par 4.1.2 fn 149. Gellman 2000 *Gov Inf Q* 235, 237 indicates the following challenges with sector-specific laws: "What constitutes a sector with enough commonality to warrant similar treatment?... Further, the line between sectors or users within sectors is not always clear enough to warrant regulation... Many record keepers have multiple lines of business that might subject them to different sectoral laws..."

Data protection legislation should cover both automatically processed data and data that are processed manually. Manually processed data cannot be excluded, because it is difficult to draw a clear distinction between the automatic and the nonautomatic handling of data – there are mixed data processing systems and there are stages in the processing of data which may or may not lead to automatic treatment.[5] Concentrating exclusively on computerised processing might also give rise to inconsistencies and lacunae, and create opportunities for record-keepers to circumvent data protection rules by using nonautomatic means for purposes which may be offensive.[6]

2.3 Public and private sector

Data protection legislation should cover both the public and the private sectors. It is no longer possible to distinguish clearly between these two sectors with regard to the processing of personal data, while the processing of data by both sectors could have equally serious implications for the data subject.[7] Data protection legislation should not be about who is doing the processing, but about protecting the privacy and identity of persons.

2.4 Natural and juristic persons

Both natural and juristic persons should be protected by a data protection regime. Most international

5 Ongoing technological developments, eg semi-automated methods based on the use of microfilm, or microcomputers which may increasingly be used for private purposes that are both harmless and impossible to control, further complicate matters (see ch 3 par 2.2.4).

6 See ch 3 par 2.2.4. According to Burkert 1986 *Computer L & Prac* 155, 157 the controversy of whether to include manual files seems to be a bit outdated and the main problem is rather how to include or exclude word processing, personal computers, distributed processing and complex databases. Seventeen years later one can add the use of personal information on the Internet to his list.

7 Simitis 1995 *Iowa L R* 445, 452 explains this proposition as follows:

> Patients in a private clinic are, as far as the use of their data is concerned, in the same situation as those treated in a hospital belonging to the state. Employees are confronted by the same problems with respect to their data whether they are employed by a computer firm or by a tax authority. The implications of processing for customers do not change because a bank is ... owned by the state and organized in a form typical of state activities.

documents and laws studied apply to individuals only.[8] However, it is submitted that it is theoretically sound in the South African law context, which recognises that juristic persons have a right to privacy,[9] to include them as data subjects under a data protection regime.[10]

Apart from the fact that it is theoretically sound to recognise juristic persons as data subjects, it stands to reason that data protection principles should also apply to them. Moreover, it may sometimes be difficult to distinguish between data relating to an individual and data relating to a juristic person, especially in the case of small companies where data relating to the company may also concern its owner(s) and provide information of a more or less sensitive nature.[11]

2.5 Exemptions from scope of legislation

Provision should be made for exemptions in instances of processing of an innocent nature, that is processing that does not pose a serious risk of infringement of privacy or identity, such as processing by natural persons for personal or domestic purposes.[12]

3 DATA PROTECTION PRINCIPLES

Data protection legislation should give effect to all ten core data protection principles,[13] namely (a) fair

8 See ch 2 par 4.2.2.3 and par 4.3.2.2; ch 3 par 2.2.4 and par 4.2.3; ch 4 par 4.3.3 and ch 5 par 4.3.3.

9 See ch 7 par 2.5.2 and ch 8 par 2.1.2 and 3.1.3.

10 See ch 7 par 2.5.2 for a discussion of the position of juristic persons as data subjects.

11 See OECD Guidelines Explanatory Memorandum 24; Gassmann "Privacy implications of transborder data flows" 109; Turn *Transborder data flows* 813.

12 See eg the Directive's provisions in this regard (ch 3 par 4.2.3).

13 See ch 6 par 2.2 for a discussion of these principles. Also see Bennett *Regulating privacy* 101–111; Gellman 2000 *Gov Inf Q* 235. Also see the Data Protection Working Party's guidance on when a data protection regime provides "adequate protection" (ch 3 par 4.2.7).

and lawful processing,[14] (b) purpose specification, (c) minimality, (d) data or information quality, (e) disclosure limitation, (f) data subject participation, (g) openness or transparency, (h) sensitivity, (i) security and confidentiality and (j) accountability. If this is done, the general theoretical principles explained in chapter 7 will also have been complied with.[15]

Exceptions could be made to the principles of purpose specification, openness or transparency and data subject participation, but these exceptions should be limited to those that are necessary in a democratic society.[16] This would include exceptions for purposes of national security; defence; public security; the prevention, investigation, detection and prosecution of criminal offences; the prevention of breaches of ethics in the regulated professions; important economic or financial interests of the State, including monetary, budgetary and taxation matters; the protection of the data subject or the rights and freedoms of others.[17] Exceptions to the data protection principles could also be allowed where data are processed for statistical purposes, or for the purposes of historical or scientific research.

In addition, the grounds for lawful processing should be stipulated. Generally, data processing should be allowed if the data subject has consented, or the processing is necessary for compliance with a legal obligation to which the controller is subject, or for the protection of the vital health interests of the data subject, or the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, or the legitimate interests of the controller or third parties to whom the data are disclosed, except where such interests are overridden by the data subject's interests in his or her right to privacy.[18]

4 SPECIAL PROVISIONS

14 This principle will be given effect to if all the other principles are achieved, and need therefore not be included *eo nomine* (see ch 6 par 2.2.1 and ch 7 par 5).

15 See ch 7 par 5.

16 See Data Protection Working Party *Transfers of personal data to third countries* 3.

17 See Dir 95/46/EC a 13. Also see ch 6 par 2.3 for a discussion of these exceptions.

18 See ch 7 par 2.3.2.3.c.

Data protection legislation should have special provisions for sensitive data, data on criminal offences, the use of a national identification number, direct marketing, automated individual decisions and freedom of expression.

Sensitive data: Additional safeguards should be in place for the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.[19] One example would be the requirement that if the data processing is based on the consent of the data subject, such consent must be given explicitly.[20]

The processing of **data on criminal offences and convictions** should be carried out under the control of an official authority, unless an exception is specifically provided for, for example for journalists or employers.[21]

National identification number: Special provisions for the use of a national identification number should also be in place to ensure that the number is not misused for purposes of compiling extensive dossiers on data subjects.[22]

Direct marketing: Where data are processed for the purposes of direct marketing, the data subject should be able to exercise an option to withdraw ("opt-out") from having his or her data used for such purposes at any stage.[23]

---

19 See the Directive's provisions (ch 3 par 4.2.4.3).

20 See Data Protection Working Party *Transfers of personal data to third countries* 4. Also see ch 4 par 4.3.4.2; ch 5 par 4.3.4.2 and ch 6 par 2.4.1.

21 See ch 3 par 4.2.4.3; ch 4 par 4.3.4.2; ch 5 par 4.3.4.2 and ch 6 par 2.4.2.

22 See ch 3 par 4.2.4.3; ch 4 par 4.3.4.2.a.iii; ch 5 par 4.3.4.2.a and ch 6 par 2.2.8.

23 See Data Protection Working Party *Transfers of personal data to third countries* 4. Also see ch 4 par 4.3.5.3; ch 5 par 4.3.8.3; ch 6 par 2.2.6 and ch 7 par 2.3.2.3.b.i.

Automated decision making / profiling: Where the purpose of the transfer of data is the taking of an automated decision, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.[24]

Freedom of expression: The processing of personal data solely for journalistic purposes or the purpose of artistic or literary expression should also be subject to special provisions. For example, it is acceptable to make exemptions or derogations from the provisions relating to the lawfulness of processing if they are necessary in order to reconcile the right to privacy with the rules governing freedom of expression.[25]

5 ENFORCEMENT MECHANISMS

5.1 Introduction

Any data protection legislation should provide for a system of external supervision. The purpose of external supervision of data protection is threefold:[26]

- ❒ to deliver a satisfactory level of compliance with the rules contained in the data protection legislation
- ❒ to provide support and help to data subjects in the exercise of their rights
- ❒ to provide appropriate redress to prejudiced data subjects where rules are not complied with

The best way of providing external supervision is through an independent data protection authority, as well as by providing data subjects with legal remedies which they can enforce in a court of law. Data subjects should be under an obligation to notify the data protection authority of any processing of

24 See Data Protection Working Party *Transfers of personal data to third countries* 4. Also see ch 4 par 4.3.5.4 and ch 5 par 4.3.8.4; ch 6 par 2.2.6.

25 See provisions of the Directive (ch 3 par 4.2.4.4; and see ch 6 par 2.3.7).

26 See Data Protection Working Party *Transfers of personal data to third countries* 4–5.

personal data before they undertake such processing, and codes of conduct should be in place for specific sectors that process data.

5.2 Data protection authority

It is evident from the study of the situation in the USA in particular that data protection legislation should make provision for an independent data protection authority to oversee all data processing activities.[27] Such an authority should have investigative powers, effective powers of intervention, and the power to engage in legal proceedings where the national data protection legislation has been violated. The data subject and controller should have the right to appeal to the courts against a decision by the supervisory body. The supervisory body should have as one of its functions the duty to hear any person's complaint concerning the protection of that person's rights in regard to the processing of personal data, as well as complaints with regard to checks on the lawfulness of data processing. The supervisory authority should also report publicly on its activities at regular intervals. Members and staff of the supervisory authority must observe a duty of confidentiality, even after their employment has ended, with regard to the confidential information to which they have had access.[28]

5.3 Notification of data processing

Data controllers must be under an obligation to furnish certain information to the data protection authority, which information should be published in a register of processing operations. Data controllers should also supply data subjects with certain information.[29]

---

27 See ch 2 par 4.2.3. Gellman 2000 *Gov Inf Q* 235, 236 states that the "two most important characteristics of successful privacy agencies are specialization and independence.... Independence is important because a privacy agency must be able to criticize the government that created it". Selmer "Data protection policy" 20 describes the principle of independence thus: "The [data protection authority] ought to have an absolute freedom to look into all parts of administration, and to state his view in public. If he is given the competence to interfere, he should have the right to make his own decision in the first instance, but his decision should be open to review on political and legal grounds".

28 See Directive's provisions (ch 3 par 4.2.5.2). Also see ch 4 par 4.3.9.1 and ch 5 par 4.3.11.1.

29 See ch 6 par 2.5.2.2.

A data controller or its representative must notify the supervisory authority before carrying out any automatic (or partly automatic) processing operation intended to serve a single purpose or several related purposes. The controller must supply its name and address and those of its representative, the purpose or purposes of the processing, a description of the category or categories of data subjects and of the data or categories of data relating to them, the recipients or categories of recipients to whom the data may be disclosed, proposed transfers of data to third countries, and a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing. The notification process may be simplified or exempted in exceptional cases only.[30]

The supervisory authority must keep a register of processing operations about which it has been notified. The information contained in the notification sent to the supervisory authority must be included in the register. The register must be open for inspection to any person. Where the processing is not subject to notification, the controller or data protection authority must make the relevant information available on request.[31]

There must be a duty on data controllers to keep data subjects informed, first of all, about the identity of the controllers and their representatives, and the purposes of the processing for which the data are intended. Further information, such as the categories of data concerned, the recipients of the data, whether replies to the questions are obligatory or voluntary, the possible consequences of failure to reply, and the existence of the right of access to data and the right to rectify such data if they are incorrect, must be supplied "in so far as it is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing" in respect of the data subjects.[32]

5.4 Codes of conduct

30 See ch 3 par 4.2.4.10.a; ch 4 par 4.3.7; ch 5 par 4.3.6 and ch 6 par 2.5.2.2.

31 See ch 3 par 4.2.4.10.c; ch 4 par 4.3.7.5; ch 5 par 4.3.6.2 and ch 6 par 2.5.2.2.

32 See ch 3 par 4.2.4.5; ch 4 par 4.3.4.2; ch 5 par 4.3.7 and ch 6 par 2.5.2.2.

It is submitted that a data protection legislation should oblige the various sectors that process data to draw up codes of conduct. This would contribute to the proper implementation of the data protection provisions in each sector. The supervisory authority must have the authority to inspect draft codes drawn up by trade associations or other representative bodies and to establish whether the codes are in accordance with the national legislation.[33]

The Dutch example[34] is instructive in this regard: An organisation or organisations that plan to draw up a code of conduct may request the data protection authority to declare that, given the particular features of the sector or sectors of society in which these organisations operate, the rules contained in the code accurately reflect the data protection legislation. In other words, two factors need to be considered when testing a code of conduct: firstly whether it correctly applies the data protection legislation, and secondly, the nature of the sector in which it will apply. The purpose of a code of conduct must be to translate the legislative provisions into a practical application in the specific information sector involved. The code should be more than a repetition of the legislative provisions. The data protection authority should consider such an application only if in its opinion the persons making the request are sufficiently representative and the sector or sectors concerned are sufficiently precisely defined in the code. The code should be reviewed periodically; approval of the code should therefore be in place for a limited period only (for example, five years).

5.5 Remedies and sanctions

Persons should be entitled to a judicial remedy, in addition to any administrative remedy, for an infringement of their rights under data protection legislation. Apart from an interdict,[35] they should also be entitled to claim compensation from data controllers or data processors for damage suffered as a result of unlawful processing. These persons may be exempted from liability, in whole or in part, if they

33 See Directive's provisions (ch 3 par 4.2.5.3). Also see ch 4 par 4.3.9.1 and ch 5 par 4.3.5.

34 See ch 5 par 4.3.5.

35 See ch 7 par 2.4.4.

are able to prove that they are not responsible for the event giving rise to the damage.[36] The data protection legislation must also lay down the (criminal) sanctions to be imposed in the event of any infringement of its provisions.[37]

6 PROVISIONS REGARDING TRANSFER OF DATA TO THIRD COUNTRIES

Any data protection legislation should include a provision that prohibits the transfer of personal data to countries that do not ensure an adequate level of data protection. This does not necessarily mean that the country in question must have its own data protection legislation. All the circumstances surrounding the data transfer must be taken into account; relevant factors are the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and the country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[38]

36 See ch 7 par 2.3.3.3.a.ii. and par 5.

37 See Directive's provisions (ch 3 par 4.2.5.1). Also see ch 4 par 4.3.5.2 and 4.3.5.5 and ch 5 par 4.3.10.

38 See ch 3 par 4.2.7; ch 4 par 4.3.4.9; ch 5 par 4.3.12. Refer also to the Safe Harbor agreement between the USA and the EU (see ch 2 par 5).