

Privacy Audit Framework under the new Dutch Data Protection Act (**WBP**)

**Version 1
April 2001**

Co-operation Group
Audit Strategy

Disclaimer

This product, the Privacy Audit Framework, was developed with the greatest care by the Co-operation Group Audit Strategy, taking into consideration the legal rules of or pursuant to the *Wet bescherming persoonsgegevens* (Dutch 'Personal Data Protection Act', 2000, normally referred to as WBP) in the best possible way.

The use of this product (the Privacy Audit Framework) shall be entirely at the user's own risk as the exact meaning to be given to these legal rules is related to circumstances which could not be taken into account at the moment of the development of this product,

CONTENTS

	<u>DISCLAIMER.....</u>	<u>2</u>
<u>1</u>	<u>FOREWORD.....</u>	<u>5</u>
<u>2</u>	<u>INTRODUCTION.....</u>	<u>7</u>
<u>3</u>	<u>PRIVACY AUDIT FRAMEWORK INTRODUCTION.....</u>	<u>11</u>
3.1	INTRODUCTION.....	11
3.2	POSITIONING PRIVACY AUDIT.....	11
3.3	WBP'S OUTLINE.....	14
3.4	PRIVACY PROTECTION AS PART OF MANAGEMENT CYCLE.....	15
3.5	DEFINING, IMPLEMENTING AND ASSESSING PRIVACY POLICY.....	16
3.6	DESIGN OF PRIVACY AUDIT FRAMEWORK.....	19
3.7	CONDUCTING A PRIVACY AUDIT.....	21
3.8	PRIVACY CERTIFICATE.....	27
<u>4</u>	<u>LEGAL FRAMEWORK FOR PRIVACY PROTECTION.....</u>	<u>29</u>
4.1	CONSTITUTION.....	29
4.2	WBP DEFINITIONS.....	30
<u>5</u>	<u>LEGAL REQUIREMENTS FOR THE PROCESSING OF PERSONAL DATA.....</u>	<u>33</u>
I	INTRODUCTION.....	34
V.1	INTENTION AND NOTIFICATION.....	35
V.2	TRANSPARENCY.....	38
V.3	FINALITY PRINCIPLE.....	41
V.4	LEGITIMATE GROUND OF PROCESSING.....	43
V.5	QUALITY.....	45
V.6	DATA SUBJECT'S RIGHTS.....	46
V.7	SECURITY.....	50
V.8	PROCESSING BY A PROCESSOR.....	52
V.9	TRANSFER OF PERSONAL DATA OUTSIDE THE EU.....	53

1 Foreword

The protection of personal data affects everyone. The extent to which measures must be taken to protect personal data against misuse or improper use depends on the data's contents, the amount of data, the purpose of the processing, the processing method and the circumstances surrounding the processing operations. Additional factors such as technological developments and social and personal vision also play a role. In short, a complex whole of factors affects the method of implementing the WBP in organisations and especially in ICT facilities.

The complexity of many aspects of the WBP requires interpretation and practical day-to-day application. This practical application is also needed in order to supervise the way in which the processors (those processing personal data) deal with and use the personal data. To put this application into practice, the *College bescherming persoonsgegevens* (the Dutch Data Protection Authority, normally referred to as CBP in Dutch) has set up a co-operation group. This co-operation group has developed a set of products that allow organisations, with different levels of depth, to check primarily by themselves how their own situation relates to the WBP. The contents and meaning of these products have been further elaborated in chapter 3. The most elaborate approach (the Privacy Audit) can allow for a certificate to be issued; a privacy certificate can be issued if the audited organisation meets the defined requirements.

Endorsement

Prior to the endorsement of the Privacy Audit Framework, this product has been tested by a number of organisations on contents and usability.

This document has been endorsed at the Steering committee meeting of the Co-operation Group Audit Strategy of December 19, 2000.

Reactions

The Co-operation Group Audit Strategy welcomes any reactions to this document. Please address your reactions in writing to:

College bescherming persoonsgegevens
Attn. Co-operation Group Audit Strategy
P.O. Box 93374
NL- 2509 AJ Den Haag
E-mail: auditaanpak@cbpweb.nl

Participants in the Co-operation Group Audit Strategy

The following market parties have contributed to the co-operation group:

- BDO Camps Obers Accountants & Adviseurs;
- BESTUUR & MANAGEMENT CONSULTANTS (BMC);
- Continuity Planning Associates;
- Deloitte & Touche;
- EDP AUDIT POOL;
- Ernst & Young;
- IQUIP Informatica B.V.;
- KPMG Information Risk Management;
- Mazars Paardekooper Hoffman;
- PricewaterhouseCoopers;
- Roccade Public;
- Singewald Consultants Group.

Potential clients and users of the audit products have been involved in the development and testing process via the following umbrella organisations:

- Consumentenbond (Consumers' Organisation);
- Information Systems Audit and Control Association Nederland (ISACA-NL-Chapter);
- Koninklijk Nederlands Instituut van Registeraccountants (NIVRA) (Royal Dutch Institute of Chartered Accountants);
- Nederlandse Orde van Register EDP-auditors (NOREA) (Dutch organisation for professional IT auditors);
- Nederlandse Orde van Accountant-Administratieconsulenten (NOvAA) (Dutch Association of Accountant and Administrative Consultants);
- VNO-NCW (Confederation of Netherlands Industry and Employers);
- FNV (Dutch Trade Union Congress);
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Ministry of the Interior and Kingdom Relations);
- Ministerie van Justitie (Ministry of Justice).

The co-operation group will maintain and update where necessary the set of products, which will also be used by the CBP in exercising its supervisory task.

2 Introduction

The Privacy Audit Framework was set up to carry out Privacy Audits in organisations where personal data are processed. Privacy Audits must be carried out in careful consideration: not every organisation is initially ready to undergo a Privacy Audit. A thorough analysis to assess whether a Privacy Audit has added value for an organisation must take place in advance. This is to prevent disappointing the client with regard to the Privacy Audit's results. If the aforementioned analysis shows that a Privacy Audit has insufficient added value for the organisation at that time, then the organisation must take proper measures first. The WBP Self-assessment can be used for this purpose if so desired. The auditor can help an organisation by giving advice during the improvement process.

Organisations can have different motives to have a Privacy Audit carried out. The auditor must be informed of the client's motives. Broadly speaking, two important motives can be recognised:

1. an economic motive (primarily aimed internally);
2. a social motive (primarily aimed externally).

Economic motive

Organisations are obliged to comply with the legal requirements for the protection of personal data. Organisations must therefore convert the WBP's conditions into a satisfactory system of measures and procedures within their own organisation, within the transitional period set. It is also in the organisations' interest to prevent any sanctions and negative reports that can result from non-compliance with the act. For these reasons an organisation's management can instruct an auditor to carry out a Privacy Audit which will give the management certainty on the implementation and compliance with the act.

The CBP encourages self-regulation by organisations and via branch and umbrella organisations. An active approach by the management to implement the legal conditions within their own organisations in an adequate way fits within this framework.

Social motive

Proper compliance with the WBP's requirements can give organisations a publicity advantage with regard to the competition. Careful processing of personal data can have a positive effect on an organisation's image and therefore has commercial value. In this way, organisations can present themselves with a positive image to clients, suppliers, employees, the public and so on with regard to privacy. In these cases, organisations may consider having a Privacy Audit carried out in order to obtain a privacy certificate. Other types of reports on the Privacy Audit can also be used in a social sense.

Target group and application

The Framework was written for auditors who are responsible for the Privacy Audit's implementation. Correct use of this framework requires sufficient knowledge and skill of audits in general and IT audits in particular. The auditor must also have sufficient knowledge of the WBP. If the auditor lacks the correct legal knowledge, then the audit must be jointly set up and carried out in collaboration with a specialised legal adviser.

The Framework offers guidance to set up an audit plan. Use of an audit plan that is geared to the organisation's specific situation is essential for an effective and efficient implementation of the Privacy Audit. Application of this framework requires a thorough and well-considered judgement by the auditor at different times. The framework does not offer a tailor-made solution. Specific work programmes have to be developed on the basis of the framework.

Standards and scope

The Framework does not give any standards for the criteria that the law demands of organisations with regard to the protection of personal data. The law gives organisations the room to further detail certain legal requirements. This can be deduced from article 13 of the WBP, which states that, 'appropriate technical and organisational measures must be taken to protect personal data against loss or any form of unlawful processing.' It is not possible to state beforehand what is seen as appropriate in a specific situation.

Criteria, which must be considered when deciding whether the measures are appropriate, include:

- state of the art in technology;
- the costs of implementation;
- the risks, both regarding processing and nature and amount of data.

The auditor defines the specific test standards according to the legal conditions, taking into account the desired scope and depth of the audit, the technical ICT infrastructure and the meaning of the privacy protection measures. Next, the consultation takes place with the organisation that is being audited, after which decision-making with regard to test standards takes place. Consultation with colleague auditors and WBP legal advisers can be very useful during this stage.

The auditor bears final responsibility for the formulation of the assignment. In as far as the Privacy Audit is carried out to obtain a certificate, the scope and depth must be determined in accordance with the requirements of the certification scheme (please refer to paragraph 3.8 Privacy Certificate), as part of the formulation of the assignment.

3 Privacy Audit Framework Introduction

3.1 Introduction

The entry into force of the WBP affects all organisations that process personal data. The act concerns both automated and non-automated processing of personal data. The management must see to it that the WBP is implemented satisfactorily within the organisation. This requires purposeful implementation of the measures that must be taken in the framework of this law. The system of measures and procedures already in place for the management and security of the processing must explicitly be tested with respect to the WBP's objectives and reconsidered if necessary.

The continuation of this chapter further explains that implementation of the WBP is primarily an organisational issue and is therefore also the primary responsibility of an organisation's management. The auditor must be aware of this when communicating with the client.

The process through which proper privacy protection is achieved is not realised overnight. Organisations need time to bring about the awareness' process. The process also requires supervision. The auditor can help in this within his/her natural advisory function. It is advisable for the management who is responsible for implementation of the WBP to appoint one or more contact persons who are responsible in particular for the coordination of the measures to be taken and the evaluation of the measures, which have been taken. The personal data protection official or the security officer could be responsible for this.

3.2 Positioning Privacy Audit

The WBP establishes requirements for processing personal data and has consequences for the procedures and measures that an organisation has taken to properly protect and manage its data processing operations. The quality range for the protection of personal data (please refer to paragraph 3.7.2) is less wide than the quality range for data processing in a broad sense (reliable, efficient, effective, exclusive, integer, continuous and auditable).

The Co-operation Group Audit Strategy has developed three products to help organisations analyse the actual situation concerning the protection of personal data and implement the desired situation. These products are called Quickscan, WBP Self-assessment (possibly with review) and Privacy Audit Framework.

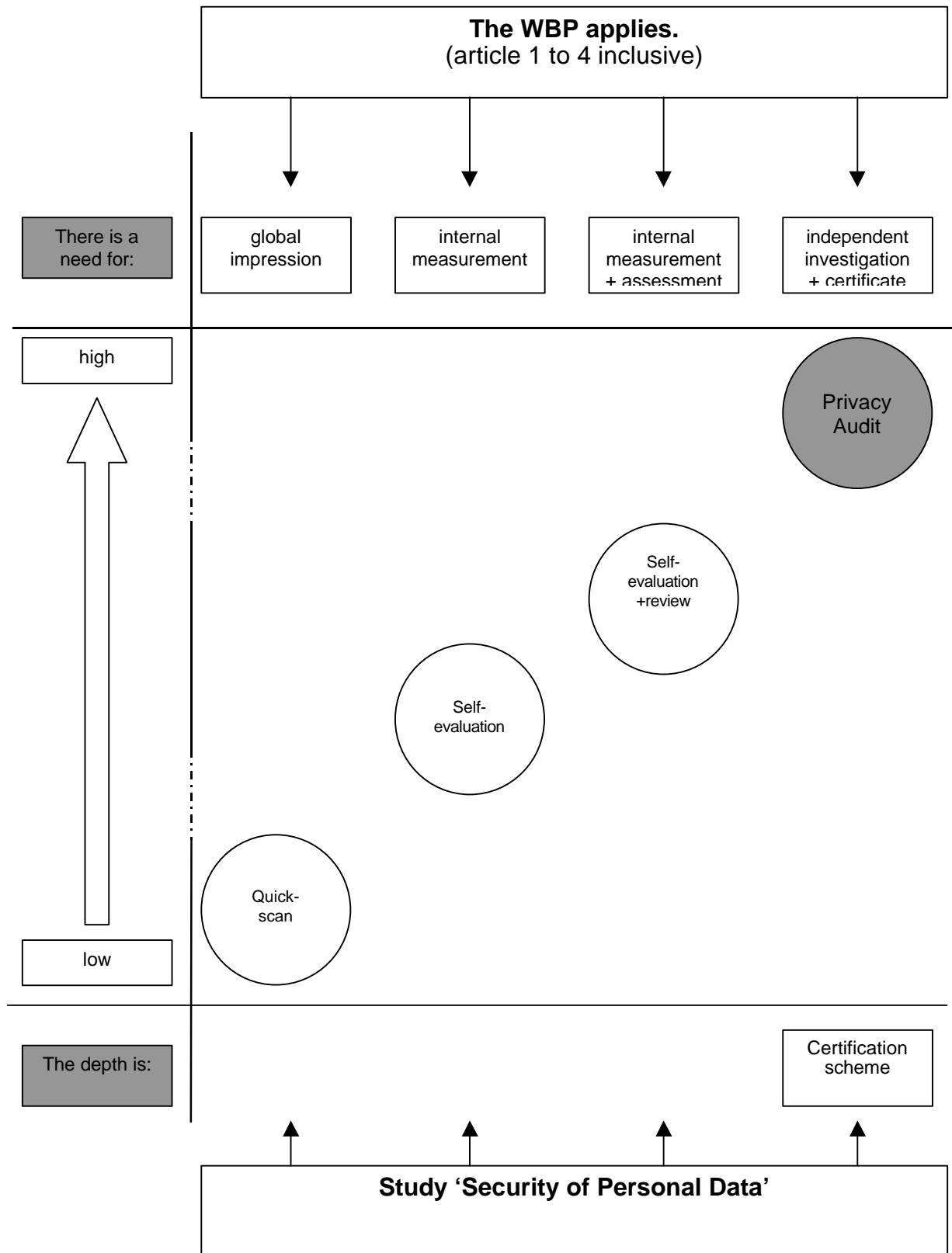
The Quickscan allows officials within an organisation to gain quick insight into the extent of awareness concerning the protection of personal data. The Quickscan's scope does not go further than creating awareness within the organisation and can be regarded as a global checklist. No statements are made as to the extent to which the WBP's conditions are met or not.

The WBP Self-assessment is a more extensive product that must be carried out by officials involved in privacy protection. The WBP Self-assessment is a systematic method for independently assessing an organisation's quality regarding privacy protection. The results of the WBP Self-assessment give a clear picture of the current situation and the necessary points of improvement. Organisations can have the internal WBP Self-assessment be reviewed by an internal or external auditor, for example an accountant or IT auditor, if so desired.

The Privacy Audit Framework forms the tailpiece of this set of products. An expert auditor/lawyer or team of experts must carry out the Privacy Audit. This is a full scope audit into the method and the extent to which the organisation meets the requirements that the law has set up for the protection of personal data.

Additionally the *Registratiekamer*, ('Dutch Data Protection Authority') the legal predecessor of the CBP, issued the 'Background study & Investigation', no. 23 'Security of Personal Data'. This study describes the necessary security measures that should be taken for the processing of personal data in different situations. This study can be ordered from the CBP.

The mutual relation between the three developed products and the study 'Security of Personal Data' is shown in the following diagram.



This document contains the Privacy Audit Framework. The diagram shows that of the products mentioned, a Privacy Audit has the most depth and is therefore the most extensive investigation.

3.3 *WBP's outline*

The WBP shall enter into force in 2001. This shall mean that the Netherlands meets the EU data protection Directive's requirement to bring the national legislation in line with this Directive. The WBP replaces the 1989 *Wet persoonsregistraties* ('Data Protection Act', abbreviated to WPR in Dutch) and comprises general legal rules to protect the privacy of citizens.

An important difference with the WPR consists of the expansion of the scope of application. The WPR mainly regulated the requirements with regard to the so-called "personal data registrations", whereas the WBP sets requirements on the entire processing chain, including collecting, recording, storing, altering, linking and consulting of personal data as well as disclosing personal data to third parties and the erasure or destruction of personal data.

The law offers citizens safeguards for careful and purpose limited processing of personal data, and gives them the possibilities to correct the processed personal data. Data subjects (those persons whose personal data are processed) can also object to the processing of their personal data. This does not mean that certain forms of processing are prohibited but the law does attach clear conditions to this.

The WBP can be summarised from two points of view:

- Legal:

The collection of personal data takes place for specified, explicit and legitimate purposes, for example with the consent of the data subject or on the basis of a legal obligation. Further processing of personal data must be compatible with the original purpose; personal data should be relevant, not excessive, adequate and accurate.

- General:

Processing of personal data offers safeguards that the right personal data are available for the right purpose, on the right grounds, for the right people at the right time.

The law distinguishes categories of personal data to which strict

conditions for use apply. This applies to the so-called 'special categories of personal data', for example data on race, political opinions, health and sex life. These personal data may only be processed by legally authorised bodies or in situations described in the law or with explicit consent from the data subject involved. The WBP does not distinguish between processing personal data by public authorities or by private business.

The WBP institutes the CBP to supervise the compliance with this privacy act. The CBP is competent (in accordance with article 60 of the WBP) to investigate the way in which the current privacy law is implemented in a given processing of personal data. When carrying out full-scale investigations, a Privacy Audit, the CBP shall use the Privacy Audit Framework as departing point.

3.4 *Privacy protection as part of management cycle*

The requirements formulated in the WBP must be implemented in the organisation in an effective way in order to guarantee the rights of citizens in an adequate way. This requires a proper system of general processing measures and procedures, that should take into account the specific protective measures necessary for processing personal data. Privacy protection will generally lead to an additional system of measures and procedures on top of the usual required processing and security measures. In order to achieve a well-balanced processing policy for personal data and to implement and maintain this properly, this policy must occupy an important place in the management cycle. Pursuing a policy that aims at protecting privacy is also in line with the management's objective of total quality and socially responsible business.

Accomplishing business objectives, via the management cycle, generally occurs via the following three phases: organisation of the processes (including policymaking), the processes themselves and assessment and adjustment of the processes. These phases are further detailed in paragraph 3.5. The working approaches and methods that lay at the basis of the development of this Privacy Audit Framework fit in with this line of thinking.

3.5 Defining, implementing and assessing privacy policy

The previous paragraph explained the importance of the privacy policy as being the responsibility of the management and part of the management cycle. A number of phases must be systematically gone through in order to define a processing policy and then implementing and maintaining it. This process is not very formalised in practice. However, this should not be an argument for the management not to have any structured approach to the process.

It is not the intention here to discuss the best method to define a processing policy and the implementation and maintenance of measures and procedures linked to this. The following explanation is aimed as guidance, focussing on the implementation of the WBP in an organisation.

Phase 1: Policy and Organisation

The starting point is to develop a privacy policy departing from the organisation's objectives, based on which a policy can be formulated for processing personal data. Additionally the existing privacy policy will be assessed and differences with regard to implementation of the WBP conditions will be mapped.

Phase 2: Processing (in terms of the WBP)

The formulated policy must give tangible form to specific measures and procedures for the processing cycle of personal data. Defining tangible measures and procedures occurs after thorough risk analysis, listing the threats which processing of personal data is exposed to. Within this context the strong and the weak points of data processing are laid down. The risks together with the strong and the weak points of the processing organisation and a cost-benefit analysis, based on the defined privacy policy, result in a carefully considered choice for the organisational and technical measures to be taken. The management is responsible for the implementation of the chosen provisions at a satisfactory level.

Phase 3: Control and Assessment (of phases 1 and 2)

Management must, with the help of a monitoring system, examine to what extent the measures taken fulfil the objectives of the formulated privacy policy. Management must indicate in what way and with which intensity it wishes to receive the monitoring data. The results of the performed monitoring form the basis for any corrective actions, adjustment of measures and procedures taken or adjustment of the

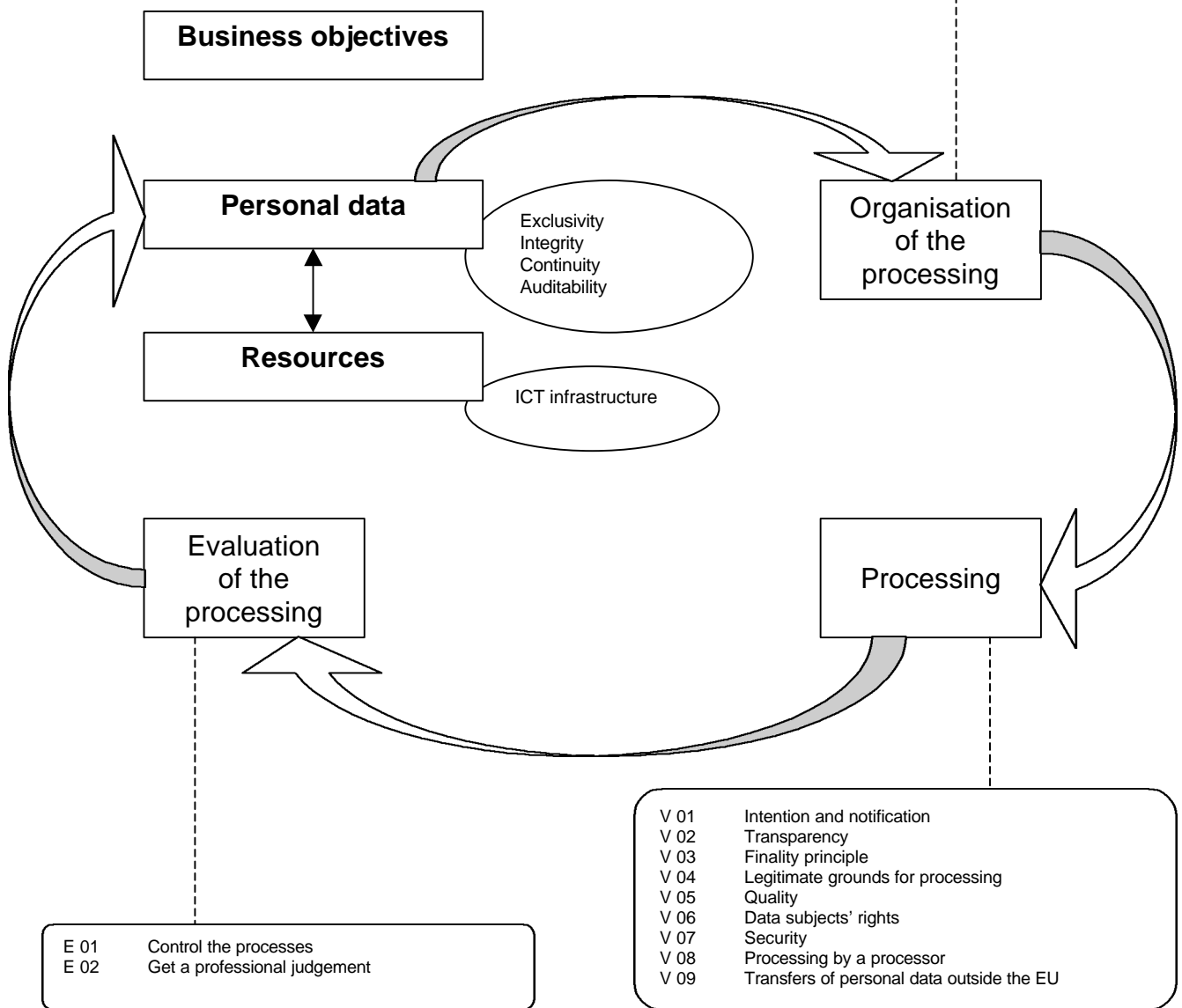
formulated policy.

The three phases of the management cycle are displayed in the following diagram. The specific detailing of the diagram's different elements has been incorporated in the Framework as follows:

- the requirements made to process personal data (V.I, V.1 to V.9 inclusive) have been described in chapter 5;
- a normative framework for the measures and procedures to be taken is displayed in appendix 2 and 3 and laid down in the earlier mentioned Study no. 23, 'Security of Personal Data'.

Note: The appendices have not (yet) been translated.

- O 01 Planning and organisation of the processing of personal data
- O 02 Define ICT infrastructure
- O 03 Set technology policy
- O 04 Define the processing organisation and its relations
- O 05 Management of quality improving processing investments
- O 06 Communicate privacy objectives and privacy policy
- O 07 Personnel management
- O 08 Ensure that additional requirements are met
- O 09 Assess dependency and vulnerability of processing
- O 10 Project management
- O 11 Quality management for the data processing
- O 12 Service level management
- O 13 Manage services of third parties
- O 14 Availability management
- O 15 Safeguard continuity
- O 16 Safeguard logical access protection
- O 17 Educate and train users
- O 18 Support and advise users (helpdesk)
- O 19 Configuration management
- O 20 Trouble shooting and incident management
- O 21 Data management
- O 22 Facility management
- O 23 Operational management



3.6 Design of Privacy Audit Framework

The essence of the Privacy Audit Framework is that by conducting the Privacy Audit, it is examined where and in which way the requirements of the WBP are already respected in the operational organisation, and which possible additional measures must still be taken to ensure a satisfactory protection of personal data.

3.6.1 Reader

The Framework gives therefore in chapter 5 (V-part) an analysis of the points of attention which must be reviewed following the WBP. For the purposes of effectiveness, examination is required of the measures taken by the organisation in order to achieve the business objectives that serve to protect personal data. In support of this analysis the appendices of this Framework show where the connection with privacy protection can be found in the organisation.

Appendix 2 Organisation of the processing (hereafter to be named the O-part) gives an explanation of the categories of measures and procedures that generally deserve attention within the organisation of processing personal data. A rather detailed explanation of possible measures and procedures is given to assist the auditor. The choice and actual implementation of measures and procedures in a specific situation within an organisation depends greatly on the current conditions within that organisation and the criteria named in the paragraph 'Standards and scope' in chapter 2. Study no. 23, 'Security of Personal Data' sketches a normative framework for the concrete detailing of measures and procedures with regard to the security of personal data. This methodology starts from a risk analysis that recognises different risk categories of personal data.

Appendix 3 Assessment of the processing (hereafter to be named part E) describes possible measures and procedures to control the processing process (see appendix 2, respectively A&V study no. 23). Appendix 4 includes a guide that shows the relation between measures and procedures from appendices 2 and 3 and the requirements, which the law lays down for processing personal data (see chapter 5).

Appendix 1 contains an overview that shows the relation between the sections of the law and the nine areas of attention. Finally, appendix 5 gives some guidance for filling in the contract between the controller and a processor and develops area of attention V.8.

3.6.2 Privacy Audit design

In chapter 5 of the Framework, the requirements arising from the legislation have been classified into nine 'areas of attention'. The implications of the legal provisions for processing personal data are discussed and laid out in that chapter. Every area of attention in chapter 5 (V-part) has implications for the detailing of the administrative organisation and measures of internal control and protection. Assessing the question of whether an area of attention is relevant and if so, to what extent attention must be paid to it in the Privacy Audit, depends on the concrete situation. Typology, nature and size of the organisation concerned as well as the nature and volume of processing personal data within that organisation play an important role in determining this.

The legal provisions have been formulated in such a way that they are applicable to all organisations and for all types of processing. Therefore no specific detailing has been given according to the typology and size of the organisation or the nature and volume of the personal data processing operations. This means that organisations will need to further define the requirements arising from the legislation specifically to their own situation. In addition to that, appropriate technical and organisational measures must be taken that provide protection against loss or unlawful processing of personal data (article 13 of the WBP) and measures and procedures that must safeguard the compliance with the other legal provisions.

In carrying out the Privacy Audit, the auditor firstly investigates whether the organisation has been set up in a way that makes possible to comply sufficiently with the legal conditions (the design). Next, the auditor assesses the existence of measures and procedures taken by the organisation in order to assure the compliance with the legal requirements. Last but not least, the auditor shall concentrate on testing the operation of the measures concerned over a predetermined period.

An organisation's management can determine the way in which technical and organisational measures are taken in order to safeguard the protection of personal data. It will try to adapt this to the existing organisation and further detailing of administrative organisational and technical measures and procedures to safeguard (automated) data processing. Based on the existing set of control instruments, the management can further implement the WBP requirements in an effective and efficient way. The law currently does not impose organisations any compulsory set up with regard to these technical and organisational measures.

It is clear that the management must take measures to comply with the WBP's requirements. To illustrate, a translation has been made in appendices 2 and 3 of the Privacy Audit Framework, based on the CobiT¹ methodology to show how the organisation can further detail and control its (automated) data processing. Via this method, the requirements that can be derived from the WBP (V-part) have been converted to concrete technical, organisational (O-part) and controllable (E-part) measures and procedures. Study no. 23, 'Security of Personal Data' shows a translation of the legal requirements to measures, based on classification of personal data in risk categories. Every choice, different to those worked out in the Framework as guide and example, is permitted for embedding WBP requirements in the organisation.

3.6.3 Framework

It has been previously mentioned that the nature and volume of personal data, the purposes of the processing and the method by which it occurs differs per organisation. This product has therefore been given the title 'Framework' as a feature. This indicates that the elaboration as given in this document is based on the most accepted common starting points of the organisational theory. Based on these starting points, it must be checked, per processing operation, to what extent the application of this Framework demands additional work or more specific detailing in relation to the object of audit.

3.7 Conducting a Privacy Audit

3.7.1 Phases

Like any audit, the Privacy Audit must be set up and carried out in a structured way to guarantee effective and efficient realisation of the audit.

Privacy Audits generally consist of the following steps:

- determine the audit assignment
- prepare the audit
- carry out the audit
- evaluate and report results

¹ Control Objectives for Information and Related Technology, 2nd edition, 1998, Information Systems Audit and Control Foundation.

3.7.2 Determine the audit assignment

The auditor and the client must reach an agreement on the assignment's goal and scope. The minimum scope of the audit is embedded in the law. Agreements must also be made as to both parties' responsibilities, realisation and the method of reporting. It is recommended that the audit assignment be laid down in writing in an assignment confirmation before commencing the audit.

In the framework of the Privacy Audit, the following quality aspects are relevant for the compliance with the requirements arising from the WBP and the compliance monitoring:

1. Exclusivity

Only authorised people have access to and can make use of personal data.

2. Integrity

The personal data must be in accordance with the projected part of reality and nothing may be wrongfully held back or made to disappear.

3. Continuity

The personal data and the information derived from this must be available without restrictions in accordance with the agreements made to that respect and the existing legal regulations. Continuity is defined as 'undisturbed progress of data processing'.

4. Auditability

Auditability is the extent to which it is possible to gain insight into the structure (documentation) and working of an object. The quality aspect of auditability also encompasses the extent to which it is possible to determine that processing personal data has been carried out in accordance with the requirements with regard to the aforementioned quality aspects.

The extent to which these aspects must be used in a concrete situation partly depends on the risk analysis performed by the auditor. The choice for quality requirements per audit object must be explained in the audit plan. The extent to which the quality aspects mentioned are relevant for obtaining a certificate will be worked out in the certification scheme.

It is possible to use a wider scope than indicated in this Framework in an assignment confirmation for a Privacy Audit. A client may want the auditor to assess the efficiency of measures and procedures taken. Such an extension of the scope does not affect the audit's fundament. Limiting the audit's scope is not permitted.

3.7.3 Preparation of the audit

Investigation of the organisation and control environment

The auditor needs insight into the organisation and control environment in order to carry out the audit effectively and efficiently. This activity forms the foundation for the audit plan to be developed in this phase.

This examination comprises in all cases the following elements:

- Organisation (knowledge of business activities, group structure, organisation diagram, information policy, privacy policy, presence of a personal data protection official);
- Organisation management (integrity, attitude with regard to privacy protection and data processing in general, use of control instruments);
- Other relevant legal requirements (specific sector-related or horizontal legislation, codes of conduct);
- Nature and volume of personal data (types of personal data, processing special categories of personal data, impact of social damage for data subjects in the event of unlawful processing);
- Organisation of the processing environment (data flows, organisation ICT infrastructure, organisation physical processing environment, administrative organisational procedures and measures).

Prior consultation with the officials involved in the protection of personal data within the organisation is advisable. Persons who can be contacted are the highest officials, the officials responsible for processing, the processor and the personal data protection official (as defined in article 62 of the WBP).

Risk analysis

Thorough risk analysis is essential in order to set up an effective and efficient Privacy Audit. The result of this analysis determines to an important extent the type and amount of control activities with respect to the technical and organisational measures in place to protect the processing of personal data. The organisation's management is expected to gear these measures to face the potential threats regarding the nature of the personal data, the volume of the processing operations and the influence of this on the social position of the data subjects in the event of unlawful processing. The CBP advises

organisations to define the system of technical and organisational measures taking into account the risk categories defined in the Study no. 23, 'Security of Personal Data'. The diagram to determine the risk categories is shown below. Please see Study no. 23 for an explanation of the diagram.

<i>Nature of the data:</i>		Standard personal data	Special categories of personal data Article 16 of the WBP
<i>Amount of personal data (nature and volume)</i>	<i>Nature of processing</i>		
Few personal data	Low processing complexity	Risk class 0	Risk class II
Many personal data	High processing complexity	Risk class I	Risk class III
Financial / economic personal data		Risk class II	

The risk analysis as part of the Privacy Audit also comprises in addition to the above-mentioned analysis an assessment of the other elements mentioned above in the paragraph 'Investigation of the organisation and control environment'.

Use of results of (different) audits

The Privacy Audit can be characterised as a regular form of auditing with its own specific scope of examination. The Privacy Audit can be fitted within the existing framework that applies to auditing financial accounts and IT audits. When carrying out the audit, the auditor can use the results of earlier audits where possible. An external auditor can also use results of investigations carried out by internal auditors, among other previous Privacy Audits for his/her own Privacy Audit.

When using results of previous audits it would be worthwhile to look at IT audits of computing centers or other processing environments within which the examined processing of personal data takes place, as well as system audits of applications with which personal data are processed. The auditor can decide, based on the audit plan and the results of these audits, which audit objects and quality aspects to use and to what extent.

Preparation of the audit results in an audit plan that concentrates on the organisation to be examined, the processing of personal data and the consecutive work programme.

3.7.4 Carry out the audit

The Privacy Audit's key activity is to examine whether the processing of personal data in an organisation complies with the WBP. The auditor must determine whether all areas of attention of part V relevant to the organisation have been sufficiently implemented. The irrelevance of one or more areas of attention must be laid down explicitly and motivated by the organisation or auditor in order to allow the correctness and completeness of this motivation to be assessed afterwards if necessary. Next, the auditor must evaluate the adequacy of the measures taken by the organisation. This requires a carefully considered professional judgement by the auditor, where necessary taken in co-operation with specific legal support.

Below follows an inventory of the aspects to which the auditor must pay attention in the framework of the assessment of the technical and organisational measures taken to guarantee a lawful processing in accordance with the requirements of the WBP.

Firstly the auditor must make an inventory of how many processing operations take place within the organisation. Chapter 2, paragraph 1 and 2 of the WBP regulates the processing of personal data. The organisation must define which types of processing there are. The examination includes the following points:

- from whom the data are obtained;
- to whom are disclosed which type of (special categories of) personal data;
- what are the data used for;
- the organisation's structure and internal and external relations;
- which information systems and types of users are distinguished;
- within which ICT infrastructure processing takes place;
- which bodies and information systems supply and receive data and the method by which this is done.

Next, the auditor must make an analysis per processing operation, paying attention to the following aspects:

- whether there is an obligation to notify;
- whether there are further requirements to process special categories of personal data;
- who is the controller and who is (are) the processor(s);
- who is (are) the internal manager(s);

- which categories of data subjects are involved;
- which type of data is or will be processed;
- what is the source of the data ;
- what are the grounds for processing;
- which categories of third parties there are
- which persons and bodies are obligated to notify the processing of personal data;
- determining the purpose of collecting the data;
- who is responsible for the audit (internal or independent auditor);
- who are the recipients of the personal data.

Measures and procedures must be specified and developed for processing personal data. Articles 6 and 13 of the WBP are at the basis of this. The auditor must assess the adequacy of these measures and procedures, among which:

- whether persons who process personal data are sufficiently aware of the problems involved;
- the obligation to notify the CBP or to the personal data protection official, article 62 of the WBP;
- the lawfulness of the processing;
- the fairness and quality of the processing of personal data;
- the transparency of the processing of personal data;
- right of access, correction and objection of the data subjects;
- ensuring that measures are kept up to date;
- ensuring the enforcement and compliance with the WBP (right of responsibility and right of inspection/audit obligation).

3.7.5 Evaluation and report results

The auditor must obtain a thorough basis to give a judgement on the extent to which the organisation complies with the legal provisions for the protection of personal data. For this purpose the auditor must collect sufficient audit evidence and lay this down in an audit file. The considerations that led to the judgement must also be laid down herein. The auditor's judgement must always be clearly formulated.

During the Privacy Audit it could emerge that specific measures, already present in the organisation, must be adjusted or that new measures must be taken to ensure that the WBP requirements are met in the given circumstances. This can be implemented through advice given to the responsible management.

3.8 Privacy certificate

Technological developments increasingly allow organisations to easily collect, record, process and use enormous amounts of data on individuals' private lives for different purposes. Attention must certainly be paid to the increasing technological possibilities to realise links between automated data files in a relatively simple way. Linking data files makes it even more difficult to trace the sources and use of data. This can give a totally different significance to personal data that at first sight appear relatively harmless. From a social point of view these developments are only accepted within certain limits. The legislator has laid down these limits in the WBP.

The importance of protecting personal data differs per organisation and depends on a large number of factors that influence each other. Examples of such factors are: the organisation's size, the nature and volume of personal data processed, the (commercial) organisation's objectives, the use of personal data to achieve that goal, the social consequences of unlawful use of personal data.

Generally speaking it is safe to say that, as the importance of the aforementioned factors increases, so does the need to protect the privacy of clients, consumers, employees and so on. With a privacy certificate, organisations can show to data subjects that they deal with the protection of their personal data with due care.

The implementation of privacy protection that is geared to the specific situation of an organisation is no sinecure. It is often assumed that certificates are by definition exclusively meant for large-scale data collection and large organisations. However a certificate can also be advisable in smaller-scale situations if personal data with a high level of risk are processed. An organisation's management must make a motivated choice. Internal and external advisors can make a useful contribution to that purpose. Interest groups can also urge an organisation's management to obtain a privacy certificate.

The import of a privacy certificate must be formulated clearly and unambiguously in order to be socially acceptable. The world that lies behind a privacy certificate is large and complex. It is therefore necessary to formulate requirements as to the meaning and contents of the certificate and to formulate requirements on the expertise of those issuing the certificate.

The Privacy Audit Framework forms the basis for issuing a certificate by a certified, independent auditor. The requirements that processing of personal data must comply with have been further detailed in a

certification scheme. The requirements for the auditor and the method by which the Privacy Audit is carried out are shown in the accreditation scheme. Both schemes will be available on the CBP website as soon as they are finalised (www.cbpweb.nl).

4 Legal framework for privacy protection

4.1 Constitution

Respecting individual privacy is one of the fundamental rights of the Dutch legal system. The right of respect to private life has been laid down in article 10 of the Dutch Constitution:

1. *With the exception of or in accordance with legal restrictions, everyone has the right to respect of his/her private life.*
2. *The law prescribes rules to protect individuals' privacy with respect to the processing and disclosing of personal data.*
3. *The law prescribes rules concerning the right of people to access data that have been processed on them and to be informed about the way in which these data are used, as well as the right to correction of such data.*

How are these principles applied in practice? Since 1989 they have been put into effect through the WPR (Data Protection Act), which contains rules for the lawful and careful handling of personal data. The WPR has been replaced by the new Data Protection Act (WBP) in 2001. This new act differs on a number of important points from the WPR. The adjustments reflect the strongly growing and still increasing possibilities of Information and Communication Technology (ICT). The main lines of the WBP are the same as those of the European Directive 95/46/EC, which was adopted on 25 October 1995. This Directive regulates how Member States must deal with the processing of personal data.

4.2 WBP definitions

The WBP brings about a number of rights and obligations. The scope of the conditions included in the WBP is to a large extent determined by the definitions included in the act. The most important definitions are shown below. (article 1 paragraph a to g of the WBP).

- a. **Personal data:** any information concerning an identified or identifiable natural person.
- b. **Processing personal data:** any operation or any set of operations concerning personal data, such as: collecting, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- c. **File:** any structured set of personal data, irrespective of whether this data set is centralised or dispersed along functional or geographical lines, that is accessible according to specific criteria and relates to different persons.
- d. **Controller:** natural person, legal person, administrative body or any other entity, which, alone or jointly with others, determines the purpose of and the means for processing personal data.
- e. **Processor:** the person who processes personal data on behalf of the controller without coming under the direct authority of that party.
- f. **Data subject:** the person to whom the personal data relate.
- g. **Third party:** Any party, other than the data subject, the controller, the processor or any person under the direct authority of the controller or the processor, who is authorised to process personal data.

The WBP uses a terminology in its definitions that could result in a lack of clarity in relation to terms used in daily practice, particularly those concerning information and communication technology (ICT). This primarily concerns the term 'processing' that is used with respect to personal data. The term 'data' in personal processing must also be clearly distinguished from the term 'data' as used in ICT jargon. To prevent misunderstandings with regard to origin and meaning of a term, the terms below shall have the following meaning within the context of this document.

WBP article	WBP context	ICT context
1 under a	Personal data	Data
1 under b	Processing personal data	Data processing
13	Security of personal data	'(Information) security'

Complete texts

The following complete texts are available on the website of the CBP:

- the WBP;
- the decree on exemption from notification;
- the decree on notification;
- the procedure to notify the processing of personal data to the Data Protection Authority.

The Ministry of Justice has published a manual on the Data Protection Act for organisations. This manual gives a clear explanation of the legal provisions and contains useful tips and guidance to help organisations when implement the legal requirements. The manual can be found at www.minjust.nl.

5 Legal requirements for the processing of personal data *(article 1, 2, 3, 4)*

The scope of the law

Article 2, first paragraph of the WBP reads:

“This act applies to the fully or partially automated processing of personal data, as well as to the non-automated processing of personal data entered in a file or intended to be entered herein.”

This article implies that processing personal data by definition does not have to fully take place within the ICT domain. Processing personal data (or parts of it) that are recorded on other media such as paper, audio or video is also included within the scope of the WBP and is therefore subject to audit during a Privacy Audit.

Framework departing point

The departing point for the Framework is that it has been determined that personal data are being processed and that this processing falls under the scope of application of the act (art. 1 to 4 inclusive of the WBP).

I Introduction (article 25, 26, 29)

The WBP provides the normative framework from which the specific technical and organisational measures for an organisation must be derived. In addition to this act regulating privacy protection in general, it can certainly be the case that other legislation and regulations are applicable, from which standards must also be derived for the organisation. The Privacy Audit assesses the compliance with all relevant legislation.

- **Decree on exemption from notification**
If a processing operation of personal data is exempted from notification, then the Decree on exemption from notification contains extra provisions, which ensue for organisations from the WBP.
- **Sector-related legislation**
These are pieces of legislation that have been developed for a specific sector and in which privacy is one of the issues regulated. Examples of sector-related legislation concern the municipal registers (Wgba), medical treatment agreements (Wgbo), police registers (Wpolr), medical examinations (Wmk) and the organization of social security (Osv).
- **Other legislation and regulations**
This refers to regulations which have effect across different sectors. The Telecommunications Act is an example of this.
- **Codes of conduct**
Certain business sectors have developed a code of conduct (article 25 of the WBP). These codes of conduct, which should be approved by the CBP, contain rules that must be used as standard in the sector for a Privacy Audit.
- **General administrative orders**
Further rules may be issued by General Administrative Order concerning the application of article 6 to 11 inclusive and 13 (art. 26 WBP). Such measures also include rules that must be used as standard for a Privacy Audit.

V.1 Intention and notification
(articles 24, 27, 28, 29, 30, 31, 32, 43)

Personal data are processed within an organisation, to which the WBP applies. The CBP or the personal data protection official must be notified of this.

During the Privacy Audit a judgement must be given on one of the following two points:

1. If an appeal has been made to an exemption for notification, then it must be decided whether this has been done on correct grounds.
2. If the CBP or the personal data protection official has been notified of the processing of personal data, then it must be determined whether the notified information corresponds with the actual situation in the organisation.

1 Determine the nature of processing and the obligation to notify

The first step is to characterise the processing operation. This step is essential to assess whether the processing operation is exempted from the obligation to notify to the CBP or the personal data protection official (article 62 and subsequently article 27 of the WBP)

Determine:

- the nature of processing;
- whether the given data processing is mentioned in the decree on exemption from notification;
- whether the processing operation corresponds with the description in the appropriate article of the decree on exemption from notification;
- the information materials of the (for example notification disk or web site) gives, after having been correctly filled in, an assessment as to whether notification must take place or not. The means which the CBP makes available for notifications, contain an overview of the processing operations exempted from notification;
- that the processing operation is exempted from the obligation to notify the CBP or the data protection official;
- that the processing operation has been notified to the CBP or personal data protection official;
- that action is taken to carry out the notification to the CBP or personal data protection official.

2 Notification

A number of matters must be known before notification takes place in the cases in which the processing operation that is not exempted from the obligation to notify. Exemption to notify does not relieve the organisation from compliance with all other provisions the WBP's. The auditor must determine that all legally required information has been included in the notification, namely:

- name and address of the controller;
- the purpose or purposes of processing;
- a description of the categories of data subjects and of the data or categories of data which relate to them;
- a description of the recipients or categories of recipients to whom data may be disclosed;
- notification of intended transfer(s) of data to countries outside the European Union;
- a general description of the technical and organisational measures which are taken to ensure the security of the personal data.
- a description of the purpose or purposes for which the data or categories of data have been collected.

3 Prior checking by the CBP

A CBP inquiry can precede the notification of the processing operation in certain cases. This is the case if:

- there is an intention to process a number to identify persons for a purpose other than for which the number is specifically intended or expressly permitted by law or general administrative order in order to link data with other data which are processed by another controller.

The following exception applies here: if the number is used for the purposes of the law which prescribe use of the number;

- there is an intention to record data based on the controller's own observation without informing the data subject;
- there is an intention to process criminal data or data on unlawful or obstructive behaviour on behalf of third parties other than in accordance with a permit on the grounds of the Private Security Organisations and Investigation Bureaus Act.

It is determined which of the above-mentioned cases is applicable. Of this is recorded:

- notification to the CBP;
- suspension of processing;

- the time when the result of the CBP inquiry is determined.

4 Central record

An overview of the notifications of processing personal data is kept at a central point in the organisation, for example with the personal data protection official. The overview shall in any case include the prescribed information for notifications and where relevant also the confirmations of receipt of the notifications to the CBP. Everyone can consult this overview free of charge.

5 Periodic assessment (exemption from) notifications

Assessments as to whether a processing operation still meets the condition for exemption and that a notification is correct will take place in the event of adjustments or periodically. The following is determined:

- a processing operation which deviates from the notification. This shall be stored for at least three years;
- whether the processing operation is more than just incidental and whether the notification to the CBP or data protection official must be supplemented and must be notified.

6 Providing information on processing

On request of any person, information will be supplied on the processing operations as it has been notified to the CBP or data protection official or on the processing operations that are exempted. The following is recorded:

- the way in which information is given relating to the processing of personal data.

If these requests are not met then it will be recorded whether this is necessary in the interest of:

- State security;
- prevention, detection and prosecution of criminal offences;
- important economic and financial interests of the State and other public bodies;
- supervising the compliance with legal regulations that are in place for one of the above-mentioned interests;
- protecting the data subject or the rights and freedoms of other persons.

V.2 **Transparency** (article 33, 34, 41, 43, 44)

Everyone must be informed about what is done with his/her personal data. The data subject must also be informed of this.

1 Providing information to the data subject

The data subject must be informed about the data processing. He/she has the right to be kept informed of the processing of his/her personal data. The following two situations can be distinguished:

1. The personal data are collected from the data subject.

Determine:

- that before the data are collected, the data subject is informed of:
 - the identity of the controller;
 - the purposes of the processing for which the personal data are intended.
- whether further information must be provided to guarantee a lawful and fair processing. Attention should be paid to the following points:
 - the nature of the personal data;
 - the circumstances in which they were collected;
 - how the data are used.

2. The personal data are collected in another manner.

Determine that the following actions have been taken at the latest at the moment when the personal data are recorded or when they are disclosed to a third party at the time of the first processing:

- the data subject shall be informed of:
 - the identity of the controller;
 - the purposes of the processing for which the personal data are intended.
- further information must be provided to guarantee a lawful and fair processing . Attention should be paid to the following points:
 - the nature of the personal data;
 - the circumstances in which they were collected;
 - how the data are used.

If the data subject is not informed, determine if:

- the data subject has already been informed of the processing;
- it is impossible or will involve a disproportionate amount of effort to inform the data subject;
 - in this case the source of the data should be recorded.
- recording or distribution occurs in accordance with the law
 - in this case information on the legal regulation concerned should be recorded.
- this is necessary in the interest of:
 - State security;
 - prevention, detection and prosecution of criminal offences;
 - important economic and financial interests of the State and other public bodies;
 - supervising the compliance with legal regulations that are in place for one of the above-mentioned interests;
 - protecting the data subject or the rights and freedoms of other persons.

2 Specificities concerning the information provision to the data subject

Determine:

- that if the organisation is an institute or service for scientific research or statistics, measures must be taken to ensure that the personal data can be used solely for scientific and statistical purposes. In that case the data subject does not have to be informed;
- whether these personal data are part of the archive records that have been transferred to a storage place in accordance with articles 12 or 13 of the Archives Act (Archiefwet 1995). In that case the data subject does not have to be informed neither.

3 Information in the case of recruitment for commercial or charitable purposes

Determine whether personal data are processed in connection with the creation or maintenance of a direct relationship between the controller or a third party and the data subject in view of recruitment for commercial and charitable purposes.

The following must be arranged:

- a direct message is sent to the data subject and in each case he/she is pointed out the possibility to object to the processing;
- the data subject must be informed of the possibilities to object to the processing if there is the intention to disclose the personal data to third parties or to use them on behalf of third parties. The announcement will be made via one or more newspapers, free local papers or in another suitable way;
- such an announcement will be made at least once a year if personal data are regularly disclosed to third parties or are used on their behalf.

V.3 Finality principle (articles 7, 9, 10)

Personal data are only collected for a specified predetermined purpose. These can be processed for that purpose and under certain conditions for other purposes.

1 Finality principle

Collection of personal data takes place for specified, explicit and legitimate purposes. Determine for which purpose the data of the examined processing operations have been collected. The information requested here can be found in V.1. Determine whether the purpose of collection has been described in sufficiently concrete terms.

2 Compatibility of the data processing

Personal data are processed in a way, which is compatible with the purpose for which the data have been collected. Determine if in the examined processing operations the purpose of the processing is compatible with the purpose of the collection. The following points must be taken into account for this assessment:

- the relation between the purpose of the intended processing and the purpose for which the data have been collected;
- the nature of the data concerned;
- the consequences of the intended processing for the data subject;
- the way in which the data have been collected and the extent to which adequate safeguards have been put in place regarding the data subject.

In the case that the processing is incompatible with the original purpose it is necessary to motivate whether this occurs on the grounds of one or more of the following exceptions:

- State security;
- prevention, detection and prosecution of criminal offences;
- important economic and financial interests of the State and other public bodies;
- supervising the compliance with legal regulations that are in place for one of the above-mentioned interests;
- protecting the data subject or the rights and freedoms of other persons;

- processing of data takes place for historical, statistical or scientific purposes. In this case the measures taken to ensure that further processing only takes place for these specific purposes must be mentioned.

3 Personal data storage

Personal data shall not be kept in a form which permits identification of the data subject for a period longer than necessary for the purposes for which they have been collected or subsequently processed. Personal data may be kept longer than provided in as far as this is for historical, statistical or scientific purposes and the necessary measures have been taken to ensure the data are only used for these specific purposes. In certain cases the storage term can also be determined by legal rules, for example the act on state taxes (Algemene Wet inzake Rijksbelastingen) or the act on medical treatment agreements (Wet Geneeskundige Behandelovereenkomst).

- Determine whether or not a (legal) storage term has been set;
- Determine whether the personal data are kept in accordance with the storage term set, or in the cases where no storage period has been fixed, whether the storage term used in practice are acceptable in view of the mentioned purposes.

4 Obligation of professional secrecy

Processing of personal data shall not occur where this is precluded by an obligation of professional secrecy by virtue of office, profession or legal regulation. Determine for the examined processing whether there is an obligation of professional secrecy and make sure that no processing takes place (outside of the professional secrecy regulations).

V.4 Legitimate ground of processing
(articles 6, 8, 16, 17, 18, 19, 20, 21, 22, 23)

Personal data may only be collected and processed if a ground for it can be found in the WBP. Specific rules apply for special categories of personal data.

1 Grounds for processing personal data

Personal data are solely processed if one or more of the following grounds apply:

- the data subject has unambiguously given his/her consent for processing;
- data processing is necessary for the performance of a contract to which the data subject is party, or in order to take pre-contractual steps which are necessary to conclude a contract at the data subject's request;
- data processing is necessary to comply with a legal obligation to which the controller is subject;
- data processing is necessary to protect the vital interest of the data subject;
- data processing is necessary for the proper performance of a task carried out in the public interest by the administrative body concerned or by the administrative body to which the data are disclosed;
- data processing is necessary for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except where the interests or the fundamental rights and freedoms of the data subject, in particular the right to protection of the private life, prevail.

Determine in which of the aforementioned cases the recorded personal data are processed. The information obtained under part V.1 serves as guideline.

2 Processing of special categories of personal data

Special categories of personal data are not processed unless the law offers a ground for this. Special categories of personal data are personal data on a person's religion or philosophical beliefs, race, political opinions, health, sex life, trade union membership, personal data concerning a person's criminal convictions and personal data on unlawful or objectionable behaviour in connection with a ban imposed with regard to such behaviour (art. 16 WBP).

Determine whether one of the above-mentioned types of data is processed. If this is the case then examine whether this is in accordance with the situations referred to in articles 17 to 23 inclusive of the WBP.

V.5 Quality
(articles 6, 10, 11)

Processing of personal data must comply with quality requirements. Quality means that the personal data are adequate, relevant, not excessive, correct and accurate in relation to the purposes for which they are collected and subsequently processed.

1 Data processing quality

Determine that the following is properly taken into account in the data processing:

- storage terms (see also V.3);
- measures for processing special (diacritical) signs;
- periodical clearing;
- information on the disclosure of corrected data to third parties to whom these data have been previously disclosed;
- final inspection for automated decisions;
- accuracy, completeness and authorisation inspection for data input (among others if inputted data are validated and processed at a point as close as possible to the source).

2 Errors in data processing

Errors are made when working with data. In order to limit errors in the data processing determine that:

- measures have been taken to minimise errors or to prevent omitting data input (among others integrity of data processing);
- there is a procedure for handling established errors (accurate, complete, in time) and for checking irregularities while drawing up basic documents, including notification;
- measures have been taken to detect and notify errors (correct and complete) during data input;
- there is a correction procedure to correct incorrect data input;
- care is taken of errors pointed out by the data subject.

V.6 Data subject's rights

(articles 5, 35, 36, 37, 38, 39, 40, 41, 42)

Persons whose data are collected have a number of rights among others the right of access, rectification, erasure, blocking and objection.

1 Implementing right of access

The data subject has the right to access his/her personal data. The following has to be arranged:

- how and where the request must be submitted;
- the data subject receives within four weeks confirmation in writing as to whether his/her personal data are processed;
- that if this is the case a full overview is provided at the same time, in an intelligent form, of the relevant personal data, a description of the purpose or purposes of the processing, the categories of data to which the processing relates, the recipients or categories of recipients and the available information as to the source of the data;
- that if a third party is expected to have objections, this third party is given the opportunity to put forward his/her view, unless an explanation is given why this is impossible or requires a disproportionate amount of effort;
- that at the data subject's request, information is given on the logic which underlies the automated processing of the data concerned;
- that, if no information is given as to the logic, it is motivated that an appeal has been made on the grounds of one or more of the following cases in the necessary interest of:
 - State security;
 - prevention, detection and prosecution of criminal offences;
 - important economic and financial interests of the State and other public bodies;
 - supervising the compliance with legal regulations that are in place for one of the above-mentioned interests;
 - protecting the data subject or the rights and freedoms of other persons.

Special circumstances can occur with requests for access. Measures have been taken so that:

- if an important interest of the requestor so demands it, the request will be complied with in a form other than in writing, taking due account of that interest;

- the request with regard to minors, who have not yet reached the age of 16 and persons placed under legal restraint, shall be made by their legal representatives. The communication concerned shall also be made to the legal representatives;
- the identity of the requestor is properly established.

2 Rectifying, supplementing, erasing or blocking

An access request can be followed by a request to rectify, supplement, erase or block personal data if they are factually inaccurate, incomplete or irrelevant for the purpose or the purposes of processing or otherwise if they are processed in conflict with a legal regulation. In that case attention should be paid to the following:

- whether the request contains the amendments to be made;
- whether the requestor is notified in writing within four weeks after receipt whether or to what extent the request is met;
- whether a refusal to a request is motivated;
- whether a decision to rectify, supplement, erase or block is carried out as quickly as possible;
- whether, where personal data have been recorded on a data carrier to which no adjustments can be made, the data user is informed about the impossibility to rectify, supplement, erase or block the data;
- whether the request with regard to minors who have not yet reached the age of 16 and persons placed under legal restraint, is made by their legal representatives. The communication concerned shall also be made to the legal representatives;
- whether, where personal data have been rectified, supplemented, erased or blocked, the third parties to whom the data have been previously disclosed, are informed as quickly as possible of the rectification, supplement, erasure or blocking, unless it has been motivated that this is impossible or shall require a disproportionate amount of effort;
- whether, when the data subject requests this, a statement is given of those parties who have been informed of the above mentioned actions.;
- whether the payment is refunded when the data are rectified, supplemented, erased or blocked on request, on the CBP's recommendation or by order of the judge.

Exception: there are public registers set up by law, which include a special procedure to rectify, supplement, erase or block data.

3 Objection

Objection means registering an objection against the processing of personal data.

3.a Relative objection

The data subject can at any time register an objection with the controller in connection his/her particular situation to the processing. This is possible in the following cases:

- data processing is necessary for the proper performance of a task carried out in the public interest by the administrative body concerned or by the administrative body to which the data are disclosed,
- data processing is necessary for the legitimate purpose of the controller or of a third party to whom data are disclosed, except where the interests or the fundamental rights and freedoms of the data subject, in particular the right to respect the private life, prevail.

The following must be arranged with regard to the objection:

- assessment as to whether the objection is justified occurs within four weeks after the request's receipt;
- if the objection is justified, processing shall be terminated immediately;
- payment of expenses in order to deal with the objection does not exceed an amount which is determined by general administrative order;
- payment is refunded if the objection is legitimate.

The aforementioned does not apply to public registers which have been set by law.

3.b Absolute objection (objection against processing for commercial or charitable purposes)

If personal data are processed in connection with creating or maintaining a direct relationship between the controller or a third party and the data subject in view of recruitment for commercial and charitable purposes, the data subject has the right to object against this processing. Such a request must always be complied with.

Determine whether the following has been arranged:

- the data subject can at any time register an objection, free of charge;
- if a direct message is sent to the data subject, he/she is pointed out the possibility to object in each case;
- measures are taken to terminate processing immediately;
- if the intention is to disclose personal data to third parties or to use them on behalf of third parties, appropriate measures must be taken to inform the data subject of the possibilities to object;
- the announcement will be made via one or more newspapers, free local papers or in another suitable way;
- if data are regularly disclosed to third parties or used on behalf of third parties, this announcement shall take place on an annual basis.

4 Automated decisions on a person's personality

Nobody may be subject to a decision which produces legal effects concerning him/her or significantly affects him/her, if that decision is based solely on the grounds of automated processing of personal data intended to gain insight in certain aspects of a person's personality. If this is the case, it must be determined why this is done. Determine whether:

- the decision has been taken in the course of entering into or performance of a contract and
 - 1. the data subject's request has been satisfied;
 - 2. the data subject has been given the opportunity to put forward his/her view.
- the ground(s) of processing is/are based on a law in which measures to safeguard the data subject's legitimate interests have been laid down;
- the data subject is informed of the logic, which underlies the automated processing of his/her data.

V.7 **Security** (articles 6, 12, 13)

The controller is under the obligation to implement appropriate technical and organisational measures to protect personal data against loss or any form of unlawful processing. The measures guarantee, having regard to the state of the art and the costs of implementation, an adequate level of security. The adequacy of the level of security depends on the risks involved in the processing and the nature of the data. The measures also aim at preventing unnecessary collection and further processing of personal data.

The CBP has developed a separate document in which the normative framework that results from art. 13 WBP has been worked out. This is Study no. 23, 'Security of Personal Data'. In this study the measures to be taken, depending on the identified risk classes of personal data, have been grouped in the following 14 categories:

1. Security policy, security plan and implementation of the system of procedures and measures
2. Administrative organisation
3. Security awareness
4. Personnel's requirements
5. Workplace design
6. Administration and classification of ICT infrastructure
7. Access management
8. Networks and external connections
9. Use of software
10. Bulk processing of data
11. Data storage
12. Data destruction
13. Contingency plan
14. Contracting out processing of personal data

The CBP stimulates the use of technical measures (Privacy-Enhancing Technologies - PET). In the cases where the choice between a technical and organisational measure exists, the Minister of Justice has shown a preference for a technical (PET) measure. The grounds for this are that a technical measure is more effective because it is harder to evade its effect.

Assess how sufficient the measures taken are and determine that these are appropriate taking into account:

- the state of the art in technology;
- the costs of implementation;
- the risks, both regarding the processing and the nature and amount of data.

Assess the weighing of organisational and technical measures by the controller in view of the statements of the Minister of Justice as phrased above.

V.8 Processing by a processor (article 14)

The controller does not process personal data, this is (partly) contracted out to the processor. This has been laid down in a contract or other legal act to create a binding agreement between the processor and the controller.

Determine whether the controller contracts out work to a processor. If this is the case then determine if there is a contract between the controller and processor and that the following has been arranged therein:

- everyone who acts under the processor's authority, as well as the processor him/herself, in as far as they have access to personal data, solely process this on instructions of the controller, except for divergent legal obligations;
- the processor complies with the obligations of the controller regarding the implementation of appropriate technical and organisational measures to protect personal data against loss or any form of unlawful processing. This concerns the measures and procedures described in chapter V.9;
- that the processor complies with the WBP and the specific legislation of that country concerning general security requirements, if the processor is established in another country of the European Union;
- for the purposes of keeping proof, the parts of the contract or the legal act relating to data protection as well as the envisaged security measures, shall be set down in writing or in another equivalent form;
- the controller checks periodically the compliance with the contract and legal provisions applicable to the processing. The processor may also periodically engage an (external) independent auditor to carry out investigation of the processing. The controller shall receive a report of the investigation carried out.

V.9 Transfer of personal data outside the EU (articles 76, 77)

Without prejudice to compliance with the act, additional rules apply to personal data which are subject to processing or which are intended to be processed in another country outside the European Union after being transferred. These data transfers are subject to rules.

Determine whether data transfer to countries outside the EU takes place.

If this is the case, attention should be paid in the investigation to the circumstances which affect the transfer of data or of a category of data. Specific attention shall be paid to the nature of the data, the purpose or purposes of the processing or processing operations and the intended storage period, the country of origin and the country of final destination, the general and sectoral legal rules in force in the third country in question, as well as the professional and security measures which are complied with in those countries.

In the cases of data transfers outside the EU, assess that:

- the country concerned ensures an adequate level of protection, or
- if the country concerned does not ensure an adequate level of protection, one or more of the following conditions is/are met:
 - the data subject has given his/her unambiguous consent;
 - the transfer is necessary for the performance of a contract between the data subject and the controller or for taking pre-contractual measures which are necessary to conclude a contract at the data subject's request;
 - the transfer is necessary for the conclusion or performance of a contract which has been or will be concluded in the data subject's interest between the controller and a third party;
 - the transfer is necessary on important public interest grounds, or to establish, exercise or defend in law any right;
 - transfer is necessary to protect the vital interests of the data subject;
 - transfer is made from a register set down by legal provisions and which can be consulted by anyone or by any person who can demonstrate legitimate interest, in as far in the case concerned the legal requirements for consultation are met.
- the Minister of Justice, after consulting the CBP, has issued a permit for a transfer or category of transfers of personal data. Transfer shall take place in accordance with the provisions attached to the permit.