GUIDELINES

FOR PERSONAL DATA PROCESSORS

PERSONAL DATA PROTECTION ACT

PERSONALDATA

TAPRO

TECTI

ONACT

Guidelines for personal data processors

Personal Data Protection Act

L.B. Sauerwein and J.J. Linnemann

Ministry of Justice

The Hague, April 2001

The electronic version of this guide and future updates are available on the website of the ministy of Justice: www.minjust.nl

P E R S O

N A L D A

T A P R O

T E C T I

O N A C T

Table of Contents

Introduction

Fast technological developments provide more possibilities to process personal data. They also offer companies, organisations and authorities more opportunities to develop new services that citizens benefit from. On the other hand, these possibilities may pose a threat to the privacy of the people involved.

A need has arisen for regulation of these and future developments. Therefore the European Parliament and the Council of the European Union adopted a European Directive. This Directive is implemented in the Netherlands by means of the *Personal Data Protection Act (Wet bescherming persoonsgegevens)*.

This new Act replaces the *Personal Data Files Act (Wet persoonsregistraties)*.

In order to assist persons, organisations, companies and government institutions that process or will process personal data in taking measures to comply with the Personal Data Protection Act, the Ministry of Justice published this guide.

This guide is not targeted at the citizens whose personal data are processed, but intended for the people, organisations, companies and government institutions that process personal data.

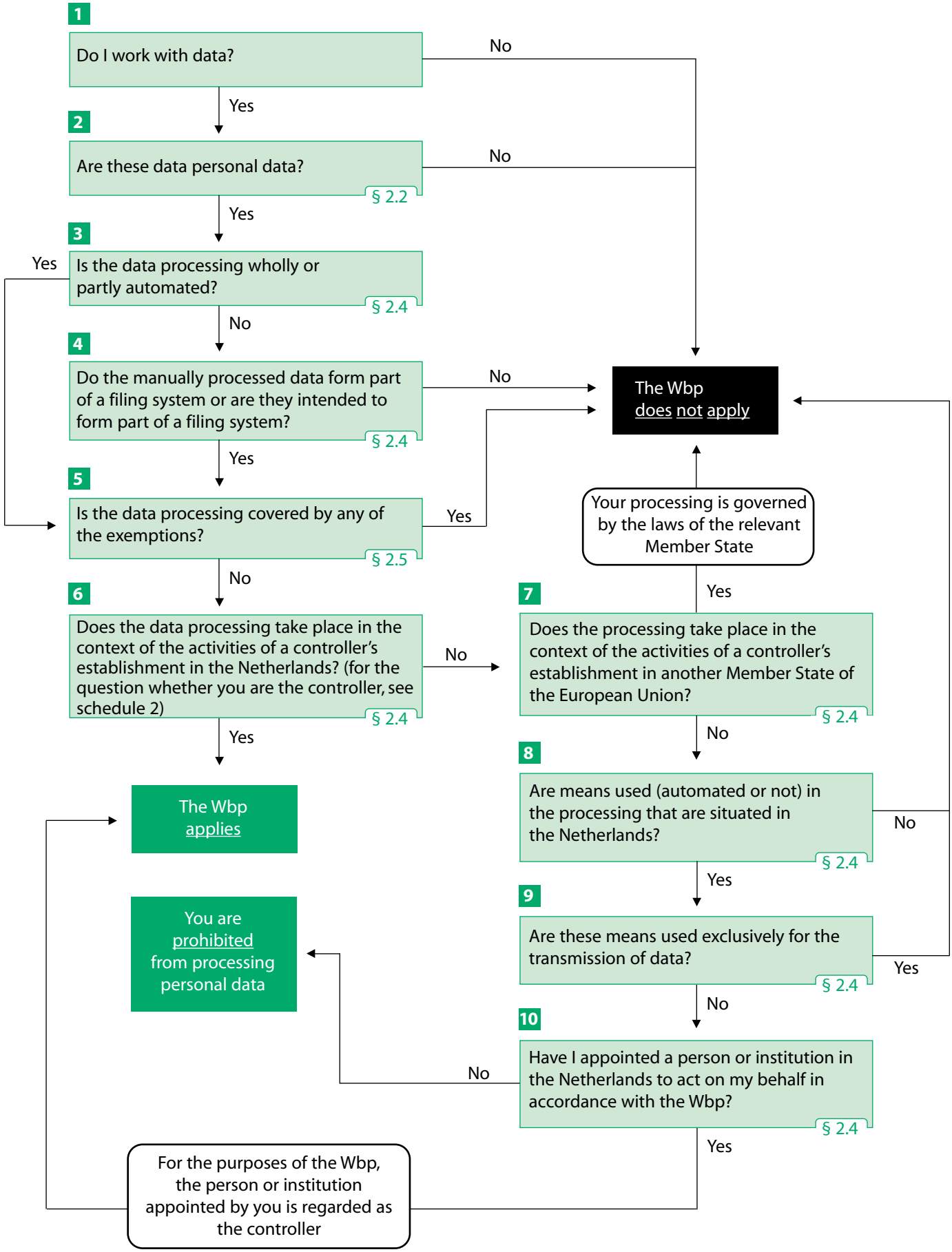
Not every section of this guide is equally relevant to all readers. By means of flow charts, we tried to direct the reader as fast as possible to those sections that are of relevance to him or her.

This guide was created in consultation with the Registration Chamber (Registratiekamer), the Confederation of Dutch Industries and Employers (VNO-NCW), the trade union FNV, the Consumers' Association (Consumentenbond), the Association of Dutch Municipalities (VNG), the Dutch Association for Direct Marketing, Distance Selling and Sales Promotion (DMSA), the Royal Dutch Medical Society (KNMG), the Dutch Bar Association (NOVA) and the Dutch Bankers' Association.

In addition to the paper edition of this guide, there is an electronic version. That version will be adapted whenever necessary, for example in the case of amendments to implementation decrees. You are therefore advised to periodically consult the electronic version. You can find it on the website of the Ministry of Justice and of the Registration Chamber or the Personal Data Protection Commission (College bescherming persoonsgegevens). The addresses can be found in the appendix to this guide.

In this guide, the Personal Data Protection Act will be referred to in brief as "Wbp", and the Personal Data Files Act as "Wpr".

Does the Wbp apply?



Controller or processor?

1

In a formal legal sense, am I the one determining the purpose and means of the processing?

Please note: you must answer this question for the legal person or organisation processing the data

§ 2.6

Yes → You are the controller

No ↓

2

Am I the one to whom the processing must be attributed according to generally accepted socio-economic standards?

Please note: you must answer this question for the legal person or organisation processing the data

§ 2.6

Yes → You are the controller

No ↓

3

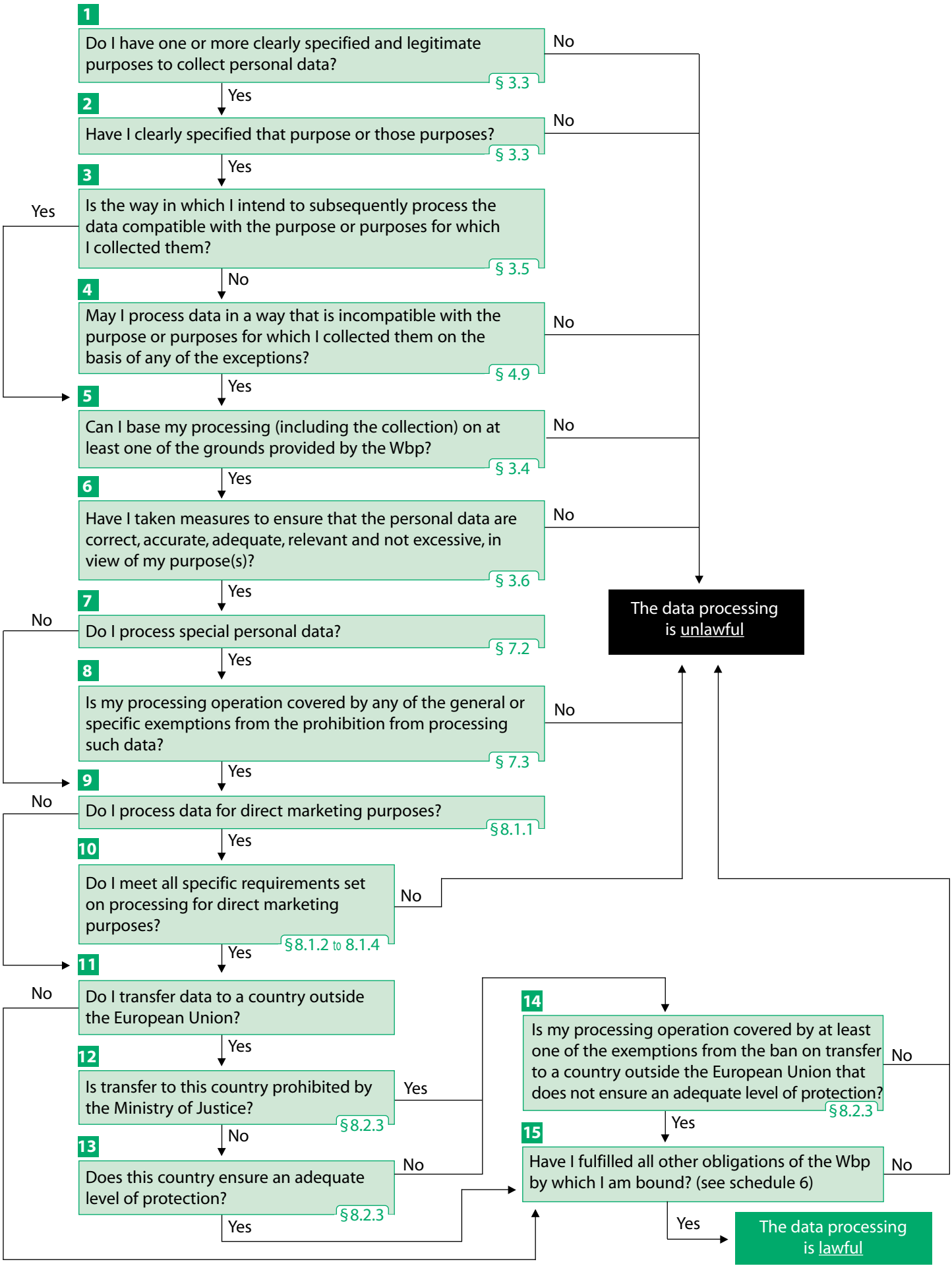
Am I under the authority of, or in a hierarchical relationship with, the party under whose responsibility I process personal data?

§ 2.7

Yes → There is internal administration. The controller is the party under whose authority you are or with whom you are in a hierarchical relationship.

No → You are a processor

Lawful processing



Notification

1 Am I processing personal data wholly or partly by automatic means? §4.2.2

- Yes → **3**
- No → **2**

2 Is my manual processing of data subject to a prior check? §4.2.2

- No → You do not have to notify your data processing
- Yes → You have to notify the Personal Data Protection Commission of your data processing

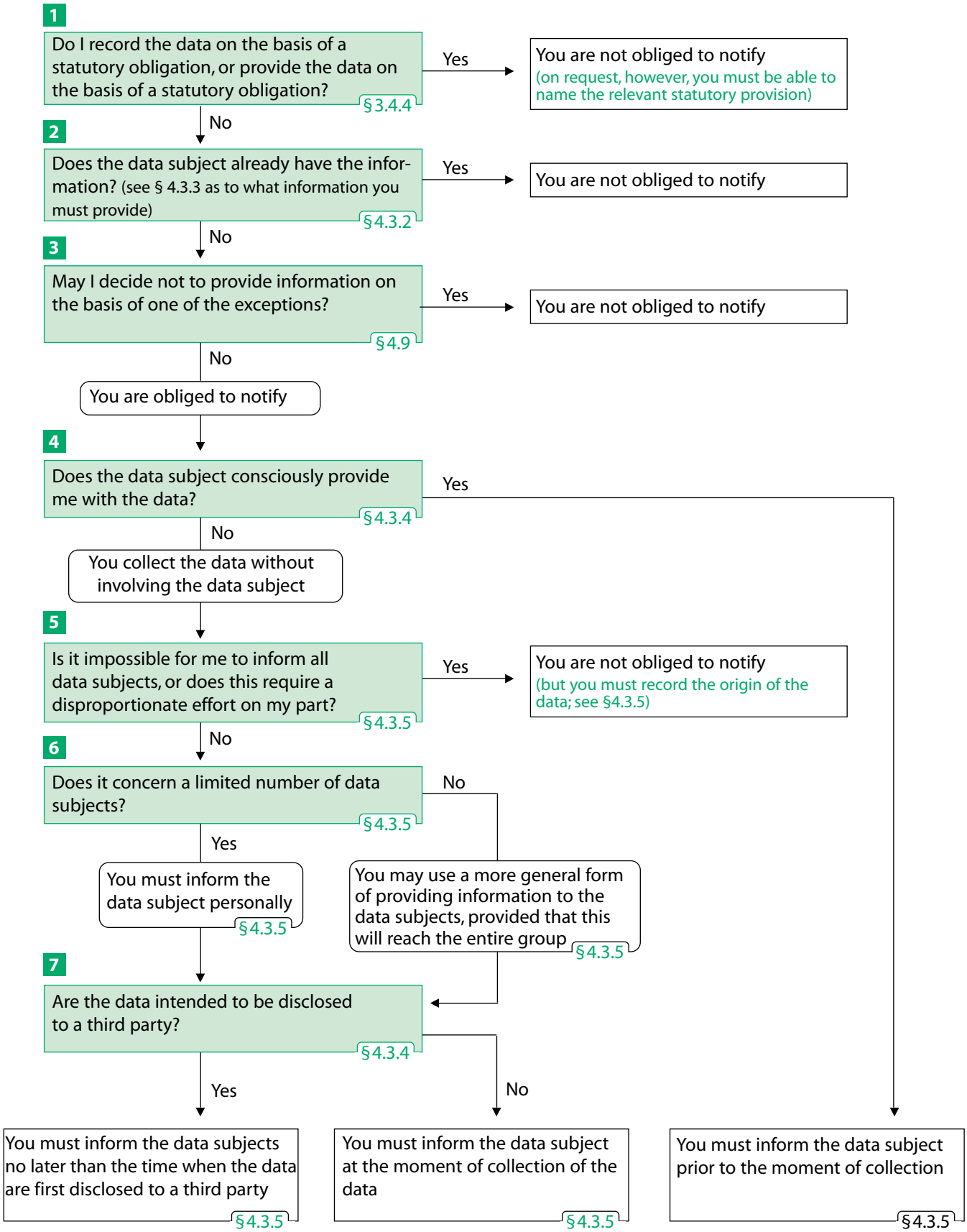
3 Is my data processing exempted from the obligation to notify? §4.2.3

- Yes → You do not have to notify your data processing
- No → **4**

4 Did I or my trade association appoint a data protection official? §6.2

- No → You have to notify the Personal Data Protection Commission of your data processing (see § 4.2.4 for the contents of the notification)
- Yes → You have to notify the data protection official of your data processing (see § 4.2.4 for the contents of the notification)

Provision of information



SEE § 4.3.3 AS TO WHAT INFORMATION YOU HAVE TO PROVIDE

The controller, the processor and the data subject: what must they do and what can they do?

The controller must:	
• Ascertain whether the data processing is lawful	→ schedule 3 lawful processing
• Ascertain whether the data processing is careful and in accordance with the Wbp and other relevant Acts	→ § 3.1 and § 3.2
• Ascertain whether it is required to notify the data processing	→ schedule 4 notification
• Secure the data processing	→ §4.6
• Not store the personal data any longer than is necessary	→ § 4.8
• Provide information to the data subject	→ schedule 5 provision of information
• Allow access to the data (at the request of the data subject)	→ § 4.4
• Correct the data (at the request of the data subject)	→ § 4.5
• End the processing of data if the data subject raises an objection	→ § 4.7 and 8.1.3
The controller can:	
• Call in a processor (the Wbp provides a number of rules)	→ § 5.2
• Appoint a data protection official	→ § 6.2
• Use the possibility of self-regulation	→ § 6.3

The processor must:	
• Process personal data solely on instructions of the controller	→ § 5.3
• Secure the data processing	→ § 5.3
• Accept the conditions which the controller must impose on the processor pursuant to the Wbp	→ § 5.3
• Maintain confidentiality	→ § 5.3

The data subject can:	
• Request access to the data	→ § 4.4
• Request correction	→ § 4.5
• Raise an objection	→ § 4.7 and 8.1.3
• Claim damages	→ § 9.2.2
• File a petition for a Court order or injunction	→ § 9.2.3
• Object to a number of decisions of the controller	→ § 9.2.4
• File a petition in connection with a number of decisions of the controller	→ § 9.2.5

Does the Wbp apply to my data processing?

2.1 Introduction

The Wbp provides rules for the *processing of personal data*. To assess whether the Wbp applies to your data processing, you will have to ascertain two things:

1 Are the data personal data?
2 Do I process personal data?

Once you have ascertained that you do process personal data, your next step is to determine:

3 Am I in control of this processing? Or: Am I the controller?

since the Wbp is primarily aimed at the *controller*.
The controller can fully or partly outsource the processing of personal data to a *processor*. The processor too is assigned certain rights and duties by the Wbp. However, not everyone who processes data for someone else is a processor within the meaning of the Wbp. If you process data for someone else, it is therefore important to determine:

4 Am I a processor?

These four questions will be dealt with in the paragraphs below.

2.2 Are the data personal data?

All data that can provide information about an identifiable natural person are personal data within the meaning of the Wbp. The Wbp refers to the person whose personal data are processed as the data subject.

personal data

Data are personal data when:

- the data contain information relating to a natural person; and
- that person is identifiable.

The data must contain information relating to natural person.

In most cases it follows from the nature of the data whether they contain information about a natural person.

factual information

- Data that by their nature provide factual information about a person.

Some data clearly provide factual information about a person. The most striking examples of this are a person's name, date of birth or sex. Data providing an evaluation of a natural person also contain information about that person. An example of this is somebody's intelligence quotient (IQ).

Some data do not relate to a person by their nature. Nevertheless, these data can be personal data, provided that the data subject is identifiable. Data that by their nature do not relate to a person are, for example:

companies or organisations

- Data concerning companies or organisations.

Data concerning companies or organisations are usually not personal data, since a company or an organisation is not a natural person. If your customer file contains only companies, the corresponding data are therefore not personal data. However, if you also record data about your contact persons in those companies, those data are personal data.

Data concerning companies or organisations can be personal data, if *they are contributory to the way in which someone is judged or treated in social and economic life.* Information about the profit of a sole proprietorship, for example, tells something in a socio-economic context about the income of the proprietor of the business. That data is in that case personal data.

items or objects

- Data concerning items or objects.

By their nature, data concerning items or objects also do not relate to a person, but can yet be personal data. Of course, the data subject must be identifiable. It depends on the context in which the data is processed whether data about an item or object is a personal data. The question at issue is again whether the data is contributory to the way in which somebody is judged or treated in a socio-economic context.

The value of a car, for example, is personal data when this data is processed in the administration of a car insurance company. As a rule, this value tells something in a socio-economic context about the income of the owner of the car. When it occurs in the price list of a car dealer, however, that value is not personal data.

identifiable

The person to whom the data relate must be identifiable.

When the data subject is not identifiable, the data is not personal data. *A person is identifiable if the person's identity can be established reasonably, without disproportionate effort.* In other words, you must be able somehow to establish a connection between the data and the person. Sometimes, the identity can be established easily. By means of name, address and date of birth, for example, it only takes a minute. Such data are called directly identifying data.

Data that have been stripped of the name can, in combination with other data or by spontaneous recognition, still lead to a certain person. In that case too, the person is - indirectly - identifiable. This depends, however, on the possibilities the controller has at his disposal. If actual identification is reasonably excluded

because of encryption of the data and/or agreements about the access to the data, the person is not identifiable. The actual situation is always the determining factor.

In conclusion: in order for data to be personal data, it must provide information about a person, either directly or indirectly. And the person must be identifiable, either directly or indirectly. This latter requirement is partly determined by the question whether the controller is actually and reasonably able to establish the identity of a person.

2.3 Do I process personal data?

Once you have ascertained that your data are personal data, the next question is whether you process personal data within the meaning of the Wbp.

processing

The processing of personal data is any operation or set of operations involving personal data.

The point is whether you can exercise any actual power or influence, whether or not by means of a computer system, over the data; you must be able to perform an operation with the data. If you cannot exercise power or influence over the personal data, you do not have to comply with the Wbp.

The Wbp mentions a number of operations that qualify as processing:

- collection, recording and organization;
- storage, adaptation and alteration;
- retrieval, consultation and use;
- disclosure by transmission;
- dissemination or otherwise making available;
- alignment and combination; and
- blocking, erasure or destruction of data.

These are just examples. Any operation with regard to personal data is processing of personal data.

In conclusion: you are processing personal data whenever you perform one or more operations relating to personal data; you must be able to exercise actual power over the personal data.

2.4 To which processing of personal data does the Wbp apply?

The Wbp does not apply to any processing of personal data. The Wbp applies to the automatic processing of personal data, as well as to some manual forms of processing.

processing by automatic means

The Wbp applies to the processing of personal data wholly or partly by automatic means.

Thus, if you store, update etc. personal data with the help of a computer, you must comply with the Wbp. The same is true if you keep your data in a cabinet, but find your way in that cabinet by means of a computer programme.

processing manually

The Wbp also applies if you manually process personal data that form part of a filing system or are intended to form part of a filing system.

"A filing system" is understood to mean a structured set of data relating to different persons. This means that

- the data must be interrelated; and
- the system must be accessible in a systematic way.

Thus, the Wbp does not cover an unstructured manual file, whereas it does cover a filing cabinet that is in any way systematized.

In addition, it is relevant where the activities involving personal data processing take place.

establishment in the Netherlands

The Wbp applies to the processing of personal data carried out in the context of the activities of an establishment of a controller in the Netherlands.

This means that an economic activity is carried out in the Netherlands by one or more establishments of a controller, in the context of which activities personal data are processed. The legal form of the controller's establishment (for example a limited liability company or a sole proprietorship) is not relevant. Branch offices are also establishments within the meaning of the Wbp.

establishment in EU

If you (as a controller) are established in *another Member State of the European Union (and not in the Netherlands),* your processing will be governed by *the law of that Member State*. This is also the case if you use means (such as telephone lines) that are located in the Netherlands for that processing.

establishment outside EU

The Wbp also applies if you process data by means of equipment situated on the territory of the Netherlands, while you are not established in the Netherlands nor in any other Member State of the European Union.

In that case, you may only process these personal data if you appoint a person or institution in the Netherlands to act on your behalf. An exception to this rule is the situation that personal data are merely transmitted by means of the above-mentioned means. This is the case, for example, with telephone lines and telecommunications equipment.

2.5 Which forms of processing are exempted; to which forms of processing does the Wbp not apply?

A number of forms of processing are explicitly exempted from the Wbp.

personal or home use

The Wbp does not apply if you process personal data solely for personal or home use.

This may be the case with personal work notes, or a tray with business cards of persons who are regularly contacted, which an employee of a company keeps as a reminder for himself. It does not matter in these cases that the employee's secretary may become acquainted with these data in special circumstances.

exempted forms of processing

The Wbp also does not apply if your data processing falls under one of the designated exempted forms of processing.

These exempted forms of data processing are:

- processing by or on behalf of intelligence or security services;
- processing for purposes of implementing police tasks;
- processing by municipalities in the municipal personal records database;
- processing for purposes of implementing the Judicial Documentation Act (Wet op de justitiële documentatie) and certificates of good behaviour; and
- processing for purposes of implementing the Electoral Provisions Act (Kieswet).

If you process personal data solely for journalistic, artistic or literary purposes, only a limited number of provisions of the Wbp apply to you.

This is a change in comparison with the Wpr. Press, television and radio now have to fulfil a number of statutory obligations in the Wbp. If you process personal data exclusively for journalistic, artistic or literary purposes, you must ensure that your data processing is proper and careful. If it is not, you may be held liable. On the other hand, you are allowed, unlike many other controllers, to process special data, such as data on criminal behaviour.

2.6 Am I the controller?

Once you have ascertained that the Wbp applies to your data processing, it is important to check whether you are the *controller.* Many obligations of the Wbp are imposed upon the controller.

controller

The controller is the party that determines the purposes and means of processing.

If you are the one who decided whether, and if yes, which data are processed, for which purpose and in which way, then you are the controller. This concerns primarily:

formal legal authority

- The party having the formal legal authority to determine the purpose and means.

So this is not the person who actually takes the decisions, not you as a manager, but the legal person, the natural person, the administrative body or any other entity that is *formally* authorized to take these decisions. That is the controller.

If these are several natural or legal persons, there is joint responsibility. This can be the case, for example, when several group companies jointly use one integrated customer file for different purposes. Those companies have joint responsibility. It is possible for those companies in such a case to assign the formal legal authority (responsibility) to one company within the corporation; the holding company, for example.

If it is not clear who has the formal legal authority or control, you should look at the second criterion:

socio-economic standards

- The party to whom the processing must be attributed according to generally accepted socio-economic standards.

It is hard to say what these socio-economic standards are; this will depend on the actual situation. This criterion was included because it is sometimes hard for citizens to determine who has the formal legal authority.

As a controller, you do not have to actually process the data yourself. What matters is whether you decide which data are processed, for how long, with which means and for which purpose. If you process data for the benefit of somebody else, you may be the processor. This is the topic of paragraph 2.7.

In conclusion: you are the controller if you are, in a formal legal sense, the party determining the purposes and means of processing. If it is not clear who has the formal legal authority, the controller is the party to whom the processing must be attributed according to generally accepted socio-economic standards.

In chapter 4 the obligations of the controller will be described.

2.7 Am I the processor?

processor

You are the processor if it is you who processes personal data *on behalf of the controller, without being under his direct authority.* Thus:

You process personal data for another party.

Your provision of service must be aimed at the execution of a certain form of processing of personal data for the benefit of the commissioner. For example, you carry out the salary administration of a company on the instructions of that

company: you are a processor. If your provision of service is aimed at something else, and if within that task you independently process the personal data of your commissioner, you are not a processor, but a controller. If, for example, you, a pension insurance company, have offered a flexible group pension scheme to a company, and that company gives you the data of the employees who take part in order to allow you to carry out this scheme, you yourself are responsible for the subsequent processing of those data.

As a processor, you have no control over the data processing, but you act on the instructions and under the responsibility of the controller. Therefore, it is your position in respect of the controller and the extent of control you have over the data processing that is decisive.

You are not under the direct authority of the controller.

If you are a subordinate, or otherwise are placed in a hierarchical relationship with, or under the direct authority of the controller, you are not a processor. In that case there is internal administration.

Here are *some examples* to explain this. You are employed by a company and you process personal data for your company: this is internal administration. Your company is the controller. When a seconded salary administrator does the salary administration for a company in that company's office, this is also internal administration. After all, the administrator works under the direct authority of the controller. If the company, on the other hand, fully outsources the salary administration to an external service agency, that agency is the processor.

In conclusion: you are a processor within the meaning of the Wbp if, when processing personal data you act in accordance with the instructions of, and under the responsibility of, a person with whom you are not in a hierarchical relationship.

In chapter 5 the obligations of the processor are described.

Which requirements must my data processing meet?

3.1 Introduction

Once you have ascertained that the Wbp applies to your data processing and that you are the controller, you must establish whether your intended data processing is also in accordance with the Wbp. The Wbp sets requirements on the processing of personal data. These requirements will be discussed in the paragraphs below. **But please note:** the Wbp is not the only Act you have to take into consideration.

Sometimes other Acts have full or partial priority over the Wbp.

Some Acts contain a *number of specific provisions* on data processing. You must meet the provisions of the specific Act regarding the subjects regulated by it, and for the rest you must meet the provisions of the Wbp. In Section 7.5 of Book 7 of the Netherlands Civil Code (on contracts in respect of medical treatment), for example, a special provision is included about (among other things) access to medical records. A physician must observe this provision whenever he allows someone access to the records. For the rest, the rules of the Wbp apply: for example, a physician may not collect more data than are necessary for his purpose.

The Wbp is aimed at both the public and the private sector.

The norms of the Wbp equally apply in the public and the private sector. The Wpr had a different regime for these sectors. In practice, the norms of the Wbp can be filled in differently for the two sectors. This has to do with the different positions of government and private undertakings in society.

3.2 My data processing must be proper, careful and in accordance with the law

The Wbp requires that you process data:

- in a proper and careful manner; and
- in accordance with the law.

properly and carefully

If you do not process data properly and carefully, you are acting unlawfully. If you do so as part of a government task (in the public sector), you are acting contrary to the principles of sound administration. What is careful in a private company is not necessarily careful in a government institution.

in accordance with the law

The requirement that data must be processed in accordance with the law means not only that you have to comply with the Wbp. As was mentioned above, you also have to observe other relevant legislation that contains special rules for data processing. Examples are Section 7.5 of Book 7 of the Civil Code, but also the Social Security Organization Act 1997 and the Telecommunications Act.

3.3 I am only allowed to process personal data for a specific purpose and based on a specific ground: what does this mean?

specific purpose

Pursuant to the Wbp, you may only collect personal data if you have a purpose for this. This purpose must be:

- specified;
- explicit; and
- legitimate.

clearly specified

You may not collect data if you have not clearly specified the purpose for which you do this. Of course, you are also allowed to collect data for multiple purposes. These purposes do not necessarily have to be related with each other.

listed and described

You must *define your purpose or purposes before you start collecting*. Therefore it is important that you carefully list and describe the legitimate purposes for which you intend to collect and process your customer data, for example. If you do not do this, you limit your possibilities. You may not simply change or extend your purposes during the processing. Under certain circumstances, however, you may further process data that you have collected for a certain purpose also for other purposes. This will be discussed in paragraph 3.5.

necessary?

When arranging your data processing, you must always ascertain whether the processing of personal data is necessary for your purpose.

This means that you must ask yourself whether you can achieve the same purpose with less data. You must also examine whether you can achieve the same result in another way, for example by using technical aids to realize that you will not process any personal data, or as few as possible.

What is required to achieve the purpose may be different in the public and the private sector. This has to do with the different roles of government and private undertakings in society.

3.4 On which grounds can I base my data processing?

3.4.1 Introduction

grounds

You must always be able to base your data processing on one of the six grounds provided by the Wbp. If you are not able to do so, you are not allowed to process personal data. Not all grounds are equally relevant to each controller. The ground dealt with in subparagraph 3.4.6 is only relevant if you belong to a government body. The other grounds can be relevant to all controllers. You may be able to base your data processing on more than one ground.

3.4.2 Unambiguous consent

unambiguous consent

The first ground for processing is processing based on the unambiguous consent of the data subject. In contrast to the Wpr, this consent no longer has to be given in writing. However, written evidence of the consent can be helpful. The consent must meet a number of criteria.

The data subject must have freely expressed his wish.

If the data subject consented to processing under pressure of the circumstances, there is no question of free will. There is also no question of free will if the data subject has a dependent position in relation to you, and consented to the processing under pressure of this dependence. For example, if an employer asks a job applicant for data on his criminal behaviour, the employer cannot say that he is processing these data with the data subject's consent.

The data subject's consent must be aimed at a specific processing or processings of data.

If the data subject has given you an unspecific authorization to process personal data, which is not aimed at specific data and specific forms of processing, this is not a legally valid consent. The consent must be aimed at the processing or set of processings intended by you. You must inform the data subject before he grants his consent in such a way that he understands what he grants his consent for. In other words, you may not assume that the data subject knows what you are going to do with the data.

The consent must be unambiguous.

You may not have any doubts about the data subject's consent. You can prevent such doubts by designing your request for consent in such a way that the consent is unambiguously clear. You may, for example, obtain a separate confirmation of the consent by having the data subject tick a box on a paper or electronic form. If you are in doubt whether an obtained consent concerns also your intended use of the data, you must find out whether the data subject gave his consent for that particular use as well.
The consent may also be apparent from the data subject's behaviour. If the data subject leaves his business card with you, a restaurant owner, in a tray destined for this purpose in order to receive mailings about new menus, his behaviour proves his unambiguous consent to the processing of personal data for that purpose.

You have to take into account that the burden of proof for obtaining the unambiguous consent is on you: you have to be able to prove that you have been granted consent, and what for. You will also have to be able to prove that this consent was granted by the free expression of the data subject's wish, and that you have informed the data subject sufficiently. Finally, you must take into

account that consent may be withdrawn at any time. Such a withdrawal will then only relate to the processing of data after the moment of withdrawal.

In conclusion: you may process data on the basis of the unambiguous consent of the data subject, provided that you have obtained this consent for a specific processing of specific data, that this consent was a free expression of the data subject's wish, that you informed the data subject about the procedure of processing, and that you have no doubts about the content and scope of the consent.

3.4.3 Necessary for the performance of a contract

performance of a contract

The second ground for processing is processing that is necessary for the performance of a contract.

If you have concluded a contract with somebody, you may use that person's personal data insofar as this is necessary for the performance of the contract.

For example, the publisher of a newspaper may process the personal data of subscribers, since this is necessary in order to allow the delivery of the newspaper. The contract does not have to be aimed at the processing of personal data, but such processing has to be a necessary consequence of the contract. You may base your processing on this ground if you are unable to perform the contract well without the personal data.

Even if you are not a party to the contract, but it is necessary that you process personal data for the performance of a contract between two other parties, this processing is allowed. The data subject himself must be a party to the contract, however. For example: the bank of the publisher of the newspaper in the example above may process the personal data of a subscriber in order to settle the payment.

precontractual phase

On the basis of this ground, you may also process data in the phase preceding the conclusion of the contract.

The processing of personal data may also be necessary in the so-called precontractual phase. You can base your data processing in the precontractual phase on this ground if:

- the data subject asks for the operations (involving the processing of personal data); and
- the operations are necessary to be able to conclude the contract.

An example of the above is the situation when a data subject asks a bank for a tender to take out a mortgage loan. The processing of personal data is necessary to be able to conclude the contract, and the data subject has asked for it.

3.4.4 The processing is necessary for compliance with a legal obligation to which the controller is subject

compliance with a legal obligation

In order to be able to base your data processing on the third ground of the Wbp, your processing must be necessary for the compliance with a legal obligation.

It has to be reasonably impossible to comply with the legal obligation without processing personal data.

There must be an obvious connection between the processing of personal data and the legal obligation. The obligation does not have to apply pursuant to a "real" Act, but may also apply pursuant to, for example a municipal regulation. This ground can only apply if you, as the controller, are yourself subject to this obligation.

An example of data processing based on this ground is the registration of employees as required by law pursuant to the Employment of Minorities Act (Wet stimulering arbeidsdeelname minderheden). Another example is the obligation to provide information pursuant to the Social Security Organisation Act 1997 (Organisatiewet sociale verzekeringen 1997).

3.4.5 The processing of personal data is necessary in order to protect the vital interests of the data subject

vital interest of the data subject

If it is necessary in order to protect a vital interest of the data subject to process his or her personal data, such processing is allowed on the basis of the fourth ground of the Wbp. This ground is mostly applied in the case of an urgent medical need. It is always preferable in any case to ask the data subject's permission. Only if this is no longer possible, for example because the data subject is unconscious, you may process personal data on this fourth ground.

3.4.6 The processing of data is necessary for the proper performance of a public law duty

public law duty

As an administrative authority, you may process personal data on the basis of the fifth ground if this data processing is necessary for a proper performance of a public law duty to be carried out by you or another administrative authority.

A public law duty is understood to mean a duty imposed by law. These are duties specifically charged to an administrative authority. For example, it is the duty of administrative authorities to treat letters of objection. In order to properly perform such duties, the administrative authority will often have to process personal data.

The data subject may register an objection against processing on the basis of this ground, in connection with his particular personal circumstances. See also paragraph 4.7 on this subject.

3.4.7 The processing of personal data is necessary for the purposes of a legitimate interest

legitimate interest

On the basis of the sixth ground, you may process personal data if this is necessary to protect the legitimate interests of you (the controller) or a third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

You must have a legitimate interest.

If you cannot perform your duties properly without processing personal data, you have a legitimate interest within the meaning of the Wbp. You do not have a legitimate interest if you already start processing data in anticipation of a future interest that is still unknown, since these data may one day come in handy.

A legitimate interest to process personal data is, for example, the sound management of your business. This does not only concern external activities, but also your internal organisation. The legitimate interest is not limited to your core activities, such as the sale of products. It may also relate to activities closely related to the core activities, such as the distribution of publicity about new products. In that case too, you have a legitimate interest.

You must be able, however, to justify the processing of personal data to an individual person. This means that you are not allowed to listen in on all your employees to find out whether trade secrets are being passed on to third parties, if only certain employees pose a risk.

necessary

Furthermore, the data processing must be necessary to your legitimate interest.

This means that you must ask yourself whether you can achieve the same result (i) with less data or (ii) in a less drastic way. In the above-mentioned example, you should examine whether you can confine yourself to listening in randomly on the employees in question.

interest of the data subject

The interests or fundamental rights and freedoms of the data subject may not be overriding in the concrete case.

With each processing, you will have to balance your legitimate interest explicitly against data subject's interest to be safeguarded from intrusions on his privacy, among other things. In such a consideration, the sensitivity of the data processed by you and the measures you took to protect the privacy of the data subject play a role. The less sensitive the data are to the data subject, and the more safety precautions you take, the bigger will be the chance that processing of personal data is allowed.

For example, if a company uses its customer file to send its customers information about a new product, that processing can be based on this ground. The marketing of new products is a legitimate interest of the company, which as a rule outweighs the limited intrusion on the privacy of the customers.

A data subject may register an objection against processing based on this sixth ground, in connection with his particular personal circumstances. This right to object will be discussed in paragraph 4.7.

3.5 My data processing may not be incompatible with the purpose for which I collected the data: what does this mean?

You collect data for a certain purpose or purposes. Of course you may then use those data for that purpose or those purposes. After you have collected the data, you may later also use them for another purpose than that for which you collected them. However, you may not do this in a way that is incompatible with the purpose for which you collected the data.

Further processing may not be incompatible. **not incompatible**

What does *not incompatible* mean? That depends on the circumstances of your specific case. The Wbp lists a number of factors, to be described below, that play a role in the determination whether a way of processing is compatible with the original purpose. Other factors can play a role too, such as the expectation a data subject has of the use to be made of his personal data. You must always take all possible factors into account and make an overall assessment. One factor does not by definition outweigh any other factor.

The Wbp lists the following factors you have to take into account in any case when you examine whether your way of further processing is compatible with the purpose for which you obtained the data. **factors**

- The extent to which a relationship exists between the original purpose and the purpose of further processing. **relationship**

The closer the two purposes are to each other (or, the more related they are), the more likely will the further processing be compatible with the purpose for which the data have been collected. The data included in file of a school on pupils, for example, may be used to map the number of graduates. But these personal data may not be sold to a company in such a form that the company can make a profile of a pupil, on the basis of which it will personally approach the pupil. The purpose for which the data have been obtained is in this case incompatible with the way in which they are processed further.

nature of the data

- The nature of the data.

The more sensitive the data are to the data subject, the less likely it will be that you may also use these data for other purposes. "Sensitive data" does not specifically refer to the *special data* (see chapter 7), but (also) to data that the data subject regards as sensitive: for example data on a minor's *placement under guardianship*.

consequences

- The consequences for the data subject of the intended (further) processing.

Particularly when further processing results in it that a certain decision is taken about the data subject, such processing will most likely be incompatible. You can think of a situation in which use of the data leads to it that the data subject is restricted in his possibilities of social development. If you are, for example, a health insurance company, and have obtained medical data about the data subject, you may not use these data as a ground for your decision whether or not to insure the life of the data subject.

way of acquiring and appropriate safequards

- The way in which the data have been acquired and the extent to which appropriate safeguards have been provided for the data subject.

If you, as an employer, can prove that in order to combat fraud it is necessary to record telephone conversations of employees without prior notice, you may not use these recordings later for the evaluation of your staff. As a rule, this way of processing is incompatible with the purpose for which you obtained the data.

The further processing for historical, statistical or scientific purposes is subject to a special provision.

Even when the data were not collected for the above-mentioned purposes, their further processing for these purposes is allowed. But in that case you have to ensure that the data will be processed for these purposes only. You may consider legal measures, such as a contract in which a scientist binds himself to use the data only for a particular purpose. Organisational or technical measures are also possible. If the result of the processing for statistical purposes is that the data are not or no longer personal data, this result may be used for all sorts of purposes, including, for example, market research.

The Wbp explicitly provides that you may not process data if this violates an obligation of secrecy by virtue of an office, administrative position, profession or statutory regulation.

Finally, the Wbp lists a number of cases in which you may process data in a way that is possibly incompatible with the purpose for which you have collected the data. For example, if the processing of personal data is necessary in the

interest of state security, or to protect the data subject or the rights and freedoms of other persons.

3.6 Which quality requirements must my data processing meet?

quality

The Wbp contains a general norm for the quality of your data processing. In view of the purpose for which they are processed, your data must be:

- adequate;
- relevant; and
- not excessive.

not excessive

You must ensure that you process sufficient and adequate data for your purpose. You may not process data that are too detailed if this is not necessary for your purpose (not excessive). If a collection agency, for example, processes data to be able to demand payment from debtors and to collect money, this purpose does not require a detailed processing of data on the products or services the debtor in question has bought. If the collection agency would do such processing, this would be excessive processing.

sufficient and adequate

On the other hand, you may not process too little data either. This means that you must process all data that are necessary (adequate) for your purpose. If you collect too little data, this may wrongly create an incomplete picture of the data subject. If the collection agency from the previous example fails to record that a debtor has been sent a credit note, an incomplete picture arises. The data processed by the collection agency are then not adequate for the purpose.

relevant

Finally, you may only process the data that are necessary for the purpose (relevant). This means you may not process superfluous data. In the same example as above, the collection agency many not always record the nationality of all debtors. After all, this is usually irrelevant to the paying of an invoice. This may be otherwise if goods of a married debtor must be attached to recover the money. In that case, the nationality may be relevant to determine which law of marital property applies.

Furthermore, the processed data must be:

correct and accurate

- Correct and accurate.

This obligation is not absolute: you do not always have to check whether the data processed by you are correct. For example, you do not have to check continuously whether all the (address) data in your customer file are still correct. But it is wise to check the data on a regular basis.

Whenever changes are made to your way of data processing, you should ask yourself whether the processing still meets the requirements described in this paragraph. In the course of time, the interpretation of your purpose may change

somewhat. In that case you must check whether the data you collect for that purpose are still adequate. If they are not, you may have to start collecting more, or possibly less, data.

What are my obligations as a controller?

4.1 Introduction

The Wbp imposes obligations on those processing personal data. These obligations rest primarily with the controller. It is true that others have obligations too, such as the processor who will be discussed in chapter 5, but those obligations are always derived from the obligations of the controller.

This chapter will describe the obligations of the controller. The obligations are described in the order of the steps you must take on the basis of the Wbp if you start collecting data now. If you are already collecting data at this moment, you do not have to read the obligations in this particular order.

All people who process personal data under the authority of a controller - this includes your employees - are obliged to treat these personal data as confidential, except where the communication of such data is required by a legal provision or is a necessity in the performance of their duties.

4.2 The notification

notification

4.2.1 Introduction

to whom do I have to notify?

As a controller, you must notify your data processing to:

- the Personal Data Protection Commission (College bescherming persoonsgegevens, the former Registration Chamber); or
- if a data protection official has been appointed by you or your trade association, you must notify to this official (see paragraph 6.2, in which this official is discussed).

If you determine the purposes and means of the processing together with others, that is, if there are several controllers, the processing can be notified by one of the controllers. Naturally all controllers will have to be mentioned in the notification.

You have to make the notification before you start processing, and therefore also before you start collecting data. The Personal Data Protection Commission will record your notification in a public register (with the exception of the information you must provide on the security of your data processing system).

Please note: You must also notify your data processing if you have drawn up regulations under the Wpr for *your registration of persons* or have already registered your registration of persons with the Registration Chamber. In that case, you must look again at all your operations involving personal data, since under the Wbp it is the *processing of* personal data you must notify.

4.2.2 Which data processing should I notify?

what must I notify?

You must notify the following:

- your processing of data wholly or partly by automatic means; and/or
- your manual processing of data, provided it is subject to a prior check.

Please note: An important group of processing operations is exempted from the duty to notify. See paragraph 4.2.3 on this topic.

processing of data

You have to notify your automated processing, and sometimes your manual processing, of data. You should bear in mind that processing operations that are regarded as a unit in a socio-economic context, are seen as one single processing operation. The Chamber of Commerce, for example, collects and stores personal data in the Commercial Register, and provides these data to third parties. In a socio-economic context, all these processing operations are seen as one unit. You should enter such a whole of processing operations in one notification. For a definition of data processing, see also paragraph 2.3.

You can enter a processing operation that serves *a single purpose or several related purposes* in one single notification. If you collect data of customers, for example, in order to fulfil customer orders, but also provide these data to third parties for direct marketing purposes, you can enter these forms of processing in one notification.

Prior checking.

manual processing

In principle you do not have to notify manual processing of data. This is only the case if your manual data processing is subject to a prior check. The legislator has named a number of data processing operations that are subject to a *prior check*. This concerns forms of processing that, in the opinion of the legislator, constitute a serious intrusion on the data subjects' privacy: for example, the collection of personal data on criminal behaviour for third parties, although the controller does not have a licence under the Private Security Organizations and Detective Agencies Act.

Before you start with these designated forms of data processing, the Personal Data Protection Commission must be able to conduct a prior check. Therefore, you must always notify such data processing to the Commission before you start it (even if you or your trade association appointed a data protection official). In this guide, we will not go further into these forms of data processing and obligations to notify.

4.2.3 Which data processing do I not have to notify? The exemptions

Exemption Decree

Many sorts of data processing are generally known to take place, and it is unlikely that that processing harms the privacy of the data subjects. You can

think for example of a staff or membership administration. The legislator deems it not necessary that all these standard forms of data processing are notified. As was the case under the Wpr, a great number of processing operations are therefore exempted under the Wbp from the duty to notify. The exempted forms of data processing are listed in the Exemption Decree (Vrijstellingsbesluit).

internet version of this guide

At the time this guide went to press, this Decree had not yet been adopted. The Internet version of this guide will be adapted as soon as possible after the adoption of the Exemption Decree. You will find the Internet version of this guide on the Internet site of the Ministry of Justice. The address can be found in the appendix to this guide.

In the Exemption Decree, several elements of the data processing are described for each type of processing:

- the purposes of the exempted forms of processing;
- the processed data or categories of data;
- the categories of data subjects; and
- the recipients or categories of recipients to whom the data are supplied.

The Exemption Decree also contains the maximum period of storing data. If you wish to make use of the exemption, your data processing must correspond to the data processing as described in the Exemption Decree in all the above-mentioned respects.

You must be prepared for it that anyone can request you to provide information about exempted forms of data processing. This could concern, for example, the purposes of your processing and the nature of the data.

The idea is to exempt those forms of processing that were exempted under the Wpr also under the Wbp from the obligation to notify. The following registrations were exempted under the Wpr, among others and on certain conditions:

- administrations of members or donors of associations or foundations;
- administrations of subscriptions;
- staff administrations;
- salary administrations;
- accounts or equivalent administrations of debtors and creditors;
- administrations of buyers and suppliers;
- administrations of pupils and students or of former members, former staff members, former pupils or former students;
- personal data files that are kept for the internal administration of the holder's organisation; and
- personal data files containing data required for communication purposes.

4.2.4 What should I do when I make a notification?

information

Your notification must include the following information:

- name of the controller (your organisation);
- address of the controller;
- purpose or purposes of the processing;
- data subjects or categories of data subjects;
- data or categories of data relating to these data subjects;
- recipients or categories of recipients;
- proposed transfers of personal data to countries outside the European Union; and
- a description of the security measures you plan to take.

The Personal Data Protection Commission prepared a standard form for the notification, which is available both in paper and electronic form. You can download this form from the Internet site of the Commission. The address can be found in the appendix to this guide.

4.2.5 What should I do when I change my data processing?

changes

If any of the following changes occurs, you must notify them within one year after your previous notification. This concerns changes in:

- the purpose or purposes of the data processing;
- the data subjects and recipients or categories of data subjects and recipients;
- the security measures; and/or
- the intended transfers to countries outside the European Union.

However, this is only required if the changes are not of a purely incidental nature. In practice, this means that you will have to check once per year whether there are any changes of a nature that is more than incidental.

In addition, you are also obliged to maintain all deviations in your data processing in respect of your notification, also if they are incidental, for at least three years. This enables you to inform the data subject of the processing, if necessary.

You must notify any change to your name or address to the Commission within one week.

4.2.6 Shouldn't I draw up regulations?

no regulations?

The Wpr made a distinction between:

- personal data files in the field of the state, education, health care and social services; and
- personal data files in the field of business and professional life, and in other fields.

With regard to the first category of registrations, the Wpr imposed the obligation to draw up regulations. Registrations in the second category had to be notified to the Registration Chamber. The Wbp only provides the obligation of the controller to notify. This notification is an extensive notification. Although the Wbp no longer contains a statutory obligation to draw up regulations, it can of course be useful to have these.

4.3 How and when should I inform the data subject about the data processing?

4.3.1 Introduction

providing information to the data subject

A person whose data are processed must be able to trace what happens with those data. Therefore, the Wbp contains a regulation on information providing to the data subject. This regulation makes a distinction in various respects between the situation in which you collect the data from the data subject himself, and the situation in which you collect the data in another way.

4.3.2 When do I not have to inform the data subject?

data subject already has the information

You do not have to inform the data subject if he already has the information described in paragraph 4.3.3.

In this respect, the Wbp is stricter than the Wpr. Your *suspicion* that the data subject has the information is not enough. You *have to know* that this is the case. But when do you know if the data subject has the information? You do not have to control whether the data subject actually read the information he was sent or given by you. After the information was sent or given, you may assume that the data subject has the information.

You may also trust that the data subject has the information if this can be deduced according to objective standards from the data subject's conduct or statement. "According to objective standards" means that anyone, not only you as a subjective person, can deduce from the data subject's conduct that he or she has the information.

You may not assume that the data subject *has the information,* if he or she (reasonably) *could have had the information.* This was the case under the Wpr, but as has been said before, the Wbp is stricter in this respect. Even if the data subject could find out, for example by research, who is the controller and for which purposes the data are processed, you must inform him or her.

4.3.3 Which information should I provide?

which information should I provide?

The information to be given to the data subject should include in any case:

- who you are (that is, who the controller is); and
- for which purpose or purposes you collect and process the data.

This does not always suffice, however. You must provide further information if that is necessary to guarantee a proper and fair processing in respect of the data subject. You will have to ask yourself whether it is necessary for reasons of due care to provide more or more detailed information to the data subject about the processing. In this respect, you must take into account (i) the nature of the data, (ii) the circumstances under which you obtained them and (iii) the use you will make of them. The more sensitive the data you processed are to the data subject, the more reason there will be to provide the data subject with detailed information about your data processing.

4.3.4 At which moment should I provide the information?

at which moment?

If you collect the data directly from the data subject, you must inform the data subject prior to the collection.

An example of collection directly from the data subject is the situation when he or she fills in personal data on a form and sends this form to you. In that case you may put the information on the form, for example. The data subject will then have the information before he returns the form (and thus before he or she provides the data).

The situation is different if you collect the data in a different way, without involving the data subject.

This is the case if you collect the data from a third party, but also if you yourself observe the data subject in his or her use of your computer network or website. In the latter case, the data subject does not consciously provide you with the data.

When data are collected without involving the data subject, you must inform him or her:

- at the moment you record the data; or
- if you collect the data exclusively to disclose these to a third party, no later than the time when the data are first disclosed to that third party.

This means that only if you collect data for the sole purpose of disclosing them to a third party, you are allowed to postpone the moment of informing the data subject to the time of first disclosure of the data. Such a third party can also be one of the companies within your group of companies. In that case, the third party does not have to inform the data subject again of the fact that he received the data.

4.3.5 How should I provide information?

You must provide the information in such a manner that the data subject can actually dispose of it.

data subject disposes of information

Therefore, a general reference to information available elsewhere is not enough. Here too, it makes a difference whether you collect the data from the data subject or without his or her involvement.

- You collect the data directly from the data subject.

In that case, you could for example include the information on the form on which the data subject provides the data (see also the previous paragraph). You could also give or send a leaflet or brochure to the data subject himself or herself. Note that this should be done before the data subject provides the data.

- You collect the data in another way; that is, not directly from the data subject.

This makes the situation more complicated: if it concerns a *limited number of data subjects,* you must inform them personally. If it concerns a whole group, you may limit yourself to a more general form of information providing. This could be by means of a bulletin or magazine (of an association, for example), provided that it is certain that this will reach the entire group of data subjects. Placing an advertisement in a national newspaper or a free local paper is not enough.

- You do not have to inform the data subject in all cases in which you collect data in another way.

It is not required if the provision of information is impossible or can only be realised by disproportionate effort. "Disproportionate effort" occurs if you can discover the data subject's address only by very time-consuming effort. In that case you are obliged to record the origin of the data, so that the data subject can in any case check later which way his data have gone. Another instance in which you do not have to inform the data subject is when you record or provide the data on the basis of a statutory obligation.

See paragraph 4.9 for other cases in which you do not have to fulfil the obligation to provide information.

4.4 When must I allow access to the data?

right to access

Anyone may ask you, at reasonable intervals, whether you process personal data relating to him, and if yes, which data. If a data subject makes such requests at an excessive frequency, you do not have to answer them.

You must answer a request for access within four weeks. The answer must be in writing, unless a vital interest of the data subject requires you to choose another form, for example an oral answer.

An answer sent by electronic mail is also a written answer. Your answer must contain the following information, in an understandable form:

- A full summary of the data of the data subject processed by you.
- A description of
  - the purpose or purposes of the data processing;
  - the categories of data to which your processing relates;
  - the recipients or categories of recipients.
- All available information about the origin of the data.

When asked, you will also have to provide information about your system of automated data processing. Of course you do not have to go as far as disclosing trade secrets.

You should make certain that the person asking for the information is really also the person about whom information is asked. If the data subject is younger than 16, or has been placed under legal restraint, the request for access must be made by his legal representative (for example a parent). In that case you will address your answer to this representative as well.

In exchange for your answer, you may charge a fee not exceeding an amount to be set by the government. The government cannot set the level of this fee above NLG 10 (€ 4,50). Only in special cases may the government set a different amount. If you corrected data on the basis of the data subject's request, you must return the fee. **Please note:** Sometimes specific Acts provide their own rules about the fee. In this respect, such Acts will take precedence over the Wbp.

In some cases you do not have to allow access to the data. See paragraph 4.9 for more information.

right to correct

4.5 When must I correct data?

The data subject is allowed to request you to correct his or her data. He or she must indicate the desired changes. Correction implies the following:

- correction;
- supplementing;
- deletion;
- blocking; or
- ensuring in another way that the inaccurate data will no longer be used.

The latter case may occur if it is technically impossible to correct the data, for example when they are stored on a CD-ROM. In that case, you have to take

other measures: including a file with supplements and corrections, for example.

when am I obliged to correct data?

You are only obliged to correct data if they are:

- factually inaccurate;
- incomplete or irrelevant to the purpose for which you process them; or
- processed in any other way that is contrary to any provision of the Wbp or other Act.

Just to be perfectly clear: your incorrect processing of the data does not have to be culpable at all.

You must inform the data subject in writing within four weeks whether, and if so to what extent, you will comply with the request for correction. If a vital interest of the person making the request so requires, you must reply differently than in writing: for example orally. If you refuse to make the correction, you have to motivate your refusal. If you decide to correct the data, you must do this as soon as possible.

notify the corrections to third parties

In case the data are corrected, you must notify the corrections to all third parties whom you provided earlier with the (inaccurate) data of the data suspect.

This is a change in comparison with the Wpr. It means you will have to examine to which third parties you provided the (inaccurate) data earlier. This duty to examine will be more far-reaching depending on how radical the corrections are, or whether the nature of the data gives rise to this. For example, if you wrongly failed to record in your system that the data subject was acquitted of a certain punishable offence he was charged with, there is more reason also to trace third parties who have been provided with incorrect data in a distant past.

impossible or disproportionate efforts

You do not have to inform third parties if:

- it is impossible for you to trace those third parties, for example since you do no longer have the information required for this; or
- this would involve a disproportionate effort on your part.

In order to determine whether an effort is disproportionate, you must weigh your interests against those of the data subject. As an example, you can think of a misspelled name in a telephone directory that is distributed nationwide. In this situation, it can hardly be required of you as the publisher of the telephone directory to inform everyone who received the telephone directory of the change. When asked, you will have to tell the data subject which third parties you informed of the change.

4.6 How should I secure my data processing?

The Wbp obliges you to secure your data processing.

technical and organisational measures

You have to implement appropriate technical and organisational measures to protect personal data against loss or unlawful processing.

Organisational measures may consist of, for example, allowing only a limited number of people access to your computer system.

appropriate level of security

The technical and organisational measures that you take must ensure an appropriate level of security.

Appropriate security means that you should take into account the following elements when choosing a security method:

- The risks involved in processing and the nature of the data to be protected.

The more sensitive the data are, the higher the applied security must be. If the data are less sensitive, you do not have to take the strongest security measures all the time.

- You must take into account the state of the art and the cost of the implementation of the measures.

If the costs of additional measures are exceptionally high in relation to the increase in the level of security, such measures are not appropriate and you do not have to take them. However, if you are able to achieve a system that is considerably more secure at a slight cost, you should certainly take such measures.

preventing unnecessary collection

The technical and organisational measures must also aim at preventing unnecessary collection or further processing of data.

Regarding the latter, you may think of the encryption of personal data, for example.

always adequate

Security must always be adequate. This means also that you will have to check periodically whether your system requires adaptation, for example due to technological developments.

The Wbp provides no concrete norms for security. In practice, standards for security have been developed. You can find out what these standards are through trade associations, for example. You will find the addresses of a number of trade associations in the appendix to this guide. When you choose your security system, you must always check whether your security meets the general norms of the Wbp, that is, whether it is appropriate and adequate.

The Personal Data Protection Commission supervises the compliance with Wbp; consequently, it also supervises whether you have secured your data processing adequately. When you call in the services of a processor, you must ensure that this processor also takes appropriate security measures. For more information, see chapter 5.

4.7 The data subject has the right to object: what should I do?

In a number of cases, the data subject can object to a processing of data. The Wbp calls this the right to object.

right to object

The data subject has the right to object if the processing of his personal data takes place on the ground that this processing:

- is necessary for the proper performance of a public law duty performed by you or by another administrative body; or
- is necessary for the legitimate interests of you (the controller) or a third party.

The data subject can register an objection on the basis of these grounds in connection with his particular personal circumstances. You as a controller (or administrative body) have to judge within four weeks after receipt of the objection whether the objection is well founded. If that is the case, you must end the processing immediately.
The data subject also has the right to object, if the processing of his personal data takes place for:

- Purposes of direct marketing.

In that case, you must always end the processing immediately. See also paragraph 8.1.3.

In exchange for the handling of the objection, you may charge a fee not exceeding an amount to be set by the government. If the objection is well founded, you have to return the fee. The data subject cannot object to the processing of his data in a public register instituted by law, such as the Land Register. Some specific Acts have separate provisions for fees, that may have precedence over the provision in the Wbp.

4.8 For how long may I store personal data?

is storage still necessary?

You may not store personal data any longer than necessary for the purpose for which you collect or (further) process the data.

It depends on the purpose for which you collected and further processed the data how long you may actually store them. This may be different in every situation; there is no fixed term for storage. You should ask yourself every time if it is still necessary for your purpose to store the data. Sometimes it can be necessary to store somebody's name on purpose, in order to make sure that no more mailings will be sent to that person, for example. What is necessary may be different in the public and the private sector. Sometimes an Act will oblige you to store data for a certain period of time.
If it is no longer necessary for your purpose to store the data, you must:

- remove the personal data; or, for example,
- remove all identifying characteristics.

You may store personal data for a longer time if this is done for historical, statistical or scientific purposes.

It does not matter in this case whether the data were originally collected for that historical, scientific or statistical purpose. You may think of the situation that you originally collected the data for a completely different purpose, but later provide them to a university for scientific research. This university may then store the personal data for a longer time, provided that it takes measures to ensure that the data are used exclusively for the scientific purpose.

With regard to specific forms of data processing that are exempted from the duty to notify, a maximum term for storage may be included in the Exemption Decree. Specific Acts may also include maximum terms for storing data, for example with regard to medical files.

4.9 Exceptions

There are a number of cases in which you do not have to fulfil some of the obligations described above. These obligations are:

- the obligation not to process your data further in a way that is incompatible with the purpose for which you obtained them (see paragraph 3.5);
- your obligation to provide information and allow access to the data (see paragraphs 4.3 and 4.4 ; see paragraph 4.3 also for other situations in which you do not have to provide information); and
- the obligation to provide information about exempted forms of data processing.

You do not have to fulfil these obligations if this is necessary:

- in the interest of state security;
- for the prevention, investigation and prosecution of criminal offences;
- for important economic or financial interests of the state and other public bodies;
- for the protection of the data subject or of the rights and freedoms of others;
- for the supervision of compliance with legal provisions established for the investigation and prosecution of criminal offences, or in the economic and financial interest of the state and other public bodies.

It has to be necessary for the protection of these interests that you do not fulfil, for example, your obligation to provide information or allow access to the data. If a request for access to the data would cause you disproportionate administrative trouble, for example, you may refuse that request for access in order to protect your interests in a proper business administration. However, the mere fact that a request for access to the data involves administrative trouble, is not in itself sufficient ground to refuse that request. In your consideration whether you are able to fulfil these obligations, you must always explicitly take the data subject's interest into account.

Finally, if you are an institution or service for scientific research or statistics you do not have to fulfil the obligation to provide information if you have not collected the data from the data subject, provided that you took the necessary measures to ensure that the personal data can only be used for statistic and scientific purposes. In that case, you may also refuse access to the data.

The Processor

5.1 Introduction

Sometimes you will not process personal data yourself, but have the actual work carried out by a specialized organisation: for example a salary administration agency. The Wbp defines the person who processes data for the benefit of the controller as the *processor.* See paragraph 2.7 on the topic of the processor.

The Wbp sets requirements on the form and content of the contracts you make with the processor. The Act also imposes a number of independent obligations and restrictions on the processor. This chapter deals with the following:

- what you have to take into account when you call in a processor; and
- which rules you have to observe if you are a processor yourself.

5.2 How do I call in a processor, and what requirements does the Act set on calling in a processor?

requirements on calling in a processor

If you decide to have the actual work involved in data processing carried out by a processor, you will enter into a relationship with that processor. The Wbp sets requirements on your choice of a processor and on the way in which you lay down your relationship with that processor:

- you must ascertain that the processor you choose provides sufficient guarantees in respect of technical and organisational security;
- you must conclude a contract with the processor or make other arrangements that create enforceable obligations between you and the processor;
- in the contract (or other arrangement), you as a controller must stipulate that the processor shall only process the personal data on your instructions;
- you must also stipulate that the processor will fulfil the security obligations incumbent on you under the Wbp (see paragraph 4.6 on the content of these security obligations); and finally
- you as a controller must actually supervise the fulfilment of these security obligations. You will have to stipulate the right to do so in the contract (or other arrangement).

The Wbp requires you to lay down in writing all parts relating to the protection of personal data and to the security measures. If you already had one or more contracts with a processor under the Wpr, you will have to examine whether these contracts need to be adapted on the basis of the provisions of the Wbp.

5.3 Which obligations does the Wbp impose on the processor?

obligations of the processor

If you process data as a processor, you are not only dealing with the requirements described in the previous paragraph, but also with obligations and restrictions which the Wbp directly imposes on the processor. These obligations and restrictions are the following.

You may only process personal data on the instructions of the controller.

This means you cannot decide of your own accord to perform a certain processing operation with the personal data entrusted to you, unless you do this in order to comply with a legal obligation.

Apart from the controller, you are independently liable for the damage or loss suffered by someone.

You are only liable to the extent that the damage is the result of your acts of processing. If you can prove that the damage cannot be attributed to you, you will not be held liable.

You and all people acting under your authority are obliged (just as the controller) to keep all personal data they become acquainted with in confidence.

What can I arrange myself on the basis of the Wbp?

6.1 Introduction

The Wbp grants you as controller a number of additional possibilities to further shape your data processing, alone or with others, and the regulations applying to it. You may, for example:

- organise internal supervision by appointing a data protection official; and/or
- set up a code of conduct, independently or for your entire line of business, in which the statutory norms for your line of business or sector are made more concrete.

6.2 The data protection official

6.2.1 Who is the data protection official?

internal supervisor

The data protection official is an internal supervisor. The official can be appointed by:

- you as a controller; or
- the trade association for your line of business; or
- another organisation to which several controllers are affiliated.

The official can only be a natural person. If you have a privacy committee in your organisation, only one of its members (or anyone else who meets the requirements to be discussed below) can assume the statutory tasks and powers of the official.

If you appoint a data protection official, your obligatory notification of a processing operation can be made to the official instead of the Personal Data Protection Commission. However, the appointment of a data protection official does not affect the powers of the Commission in any way.

6.2.2 How to appoint a data protection official?

requirements of the official

You may only appoint a person who:

- has sufficient knowledge; and
- is sufficiently reliable.

The knowledge must be knowledge of privacy legislation and of your organisation and line of business, as well as of the processing operations within that organisation and line of business

Once you appointed an official, you can no longer give him instructions as to his duties as data protection official; he must be in a position to duly exercise his functions in complete independence.

powers

You have to enable him to do so by granting him the necessary powers. These (internal) powers must be equivalent to the powers held by the supervisors of the Personal Data Protection Commission and other bodies. For example the power to:

- enter premises,
- demand information; and
- require the inspection of data and documents.

The official may not be adversely affected by the performance of his duties. For example, you may not judge the "usual" work of the official any worse than it really is in order to exert influence on his functioning as data protection official. It is likely that the data protection official will get protection against dismissal comparable to that of, for example, a member of a works council. The bill to that effect was still under discussion in Parliament at the time this guide went to press.

Finally, you will have to report the appointment of a data protection official to the Personal Data Protection Commission. The Commission keeps a list of reported officials. With the help of this list, data subjects can find out whether a certain processing of data is supervised by an official.

6.2.3 What are the duties and powers of the data protection official?

The official has a number of duties and powers.

supervision

The official must supervise that you process personal data in accordance with the statutory regulations.

Of course, his supervision will be limited to your processing of personal data. If he is appointed by an organisation of controllers, his supervision will be limited to the processing operations of the associated controllers.

It is self-evident that data subjects will turn to the official with their complaints or requests. The official is obliged to observe secrecy in respect of anything that is disclosed to him in this respect, unless the data subject gives his consent to a disclosure.

notification

The official must accept your notification and keep a register of all data processing operations that have been reported to him.

If a data processing operation is exempted from the duty to notify, you will of course not have to report this operation to the official either.

report

Finally, the official must draw up an annual report on his work and findings.

In that report, but also outside of it, he can make recommendations to achieve a better protection of the data that are being processed. Of course the official may consult with the Personal Data Protection Commission, if he wishes.

6.3 Is self-regulation by my sector possible?

code of conduct

An organisation or group of organisations, for example your branch organisation, can also adopt a code of conduct.

The code of conduct can relate to one or more sectors. In a code of conduct, the provisions of the Wbp can be made concrete and elaborated for a particular sector. The code of conduct can also include a regulation for the settlement of disputes.

statement Personal Data Protection Commission

Before you adopt a code of conduct, you may request the Personal Data Protection Commission to review the draft code and issue a statement on it.

You can also make this request if you change or renew an existing code of conduct. The Commission will only take up a request if it considers the petitioner or petitioners sufficiently representative and if the sector or sectors involved have been described with sufficient accuracy.

The Commission will judge whether the code or draft code is a correct elaboration of the Wbp or of other statutory provisions about the processing of personal data, in view of the special characteristics of your sector. If the code contains a regulation for the settlement of disputes, the Commission will only approve the code if that regulation provides sufficient safeguards for the independence of the person or body settling disputes.

The Commission will issue a statement on the code of conduct and will publish it along with the code of conduct in the Government Gazette (Staatscourant).

The Government may lay down further rules for a particular sector.

May I process special personal data?

7.1 Introduction

The nature of some personal data entails that their processing can constitute a big intrusion of the data subject's privacy, since such data contain sensitive information about someone. The Wbp refers to such data as special personal data. The processing of *special personal data* is subject to a stricter regime than the processing of ordinary personal data. In paragraph 7.2 it is explained which data are special personal data. In paragraph 7.3, the rules for processing such data are explained.

7.2 What are special personal data?

special personal data

Special personal data are all personal data that provide information on a person's:

- religious or philosophical beliefs;
- race;
- political opinions;
- health;
- sex life; and
- membership of a trade union.

Furthermore, special personal data are:

- personal data connected with a person's criminal behaviour; and
- personal data connected with unlawful or objectionable conduct for which a ban has been imposed (a street ban, for example).

An example of data connected with criminal behaviour are data about a person's convictions, but also data about the Justice Department's suspicion of a punishable offence. Data about a person's health include of course medical data, but also in general all data about a person's mental or physical health.

7.3 When is it prohibited to process special personal data and when is it allowed?

prohibition on processing, unless

The principle of the Wbp is that you may not process special personal data. The Wbp provides a number of general and specific exemptions from this prohibition.

Even if the prohibition on processing special personal data does not apply to your processing, you must still meet the other provisions of the Wbp and other applicable regulations. This means, for example, that you must have a specified, explicit and legitimate purpose for the collection of special personal data too, and that you must secure these data. If you cannot lift the ban on processing of special personal data with the help of one of the specific exemptions, perhaps one of the general exemptions applies. The general exemptions in the Wbp are actually a kind of remaining provisions. Therefore, the following subparagraphs

will first address the specific exemptions, and then the general exemptions.

In this guide, the personal data about a person's political opinions or membership of a trade union are not discussed; personal data concerning criminal behaviour are also left out.

7.3.1 Personal data about a person's religious or philosophical beliefs

religious or philosophical beliefs

In brief, the ban on processing data about someone's religious or philosophical beliefs does not apply to:

- church associations or other associations founded on spiritual principles; or
- other associations founded on spiritual or philosophical principles.

Examples of such other associations are a home for the elderly based on Islamic principles, or a Catholic university. The associations and institutions may process data on, for example, the religion of their employees or patients, of course provided that the general requirements of the Wbp for data processing have been met. The home for the elderly may, for example, collect data on the religion of its patients in order to be able to provide them with adequate spiritual care.

Church or other spiritual associations may also process data about the religious or philosophical beliefs of family members of their own members, provided that the association maintains regular contact with the family member concerned, for example once per year.

You may never provide the data about a person's religious or philosophical beliefs to third parties without the data subject's consent.

7.3.2 Personal data about a person's race

race

You may only process data about a person's race in very exceptional cases. Actually this is only allowed if you process such data for:

- identification purposes; or
- in connection with a policy of affirmative action.

In the latter case, additional conditions must have been fulfilled, for example the data subject's not having expressed any objection to it in writing.

An example of processing data for identification purposes is a system of access passes with photographs of your employees. Under certain circumstances, it is possible to deduce the race of the employee concerned from such a photograph. This form of processing is allowed if passes with photographs are inevitable to the identification of your employees, for example since the size or public accessibility of your company involves the need for identification by

means of a photograph. However, this does not mean that you are never allowed to process photographs of your employees, for example in a company directory. You may process such data if your employees gave you their explicit consent (see paragraph 7.3.4).

7.3.3 Personal data about a person's health

mental or physical health

Data about a person's health include, as was mentioned above, all data concerning the mental or physical health of a person. This includes, for example, the data that one of your employees has a heart condition. You may process such data in any case if you belong to any of the groups specified in the Wbp. You may also process such data if you have the explicit consent of the data subject, for example. This possibility is relevant especially to employers who wish to take measures for their "sick" employees. See also the general exemptions described below.

As mentioned above, the Wbp names a number of groups of controllers that may, under certain conditions, in any case process data about a person's health. However, the Wbp places restrictions on the purposes for which these groups may process health data. These groups include:

- hospitals;
- institutions for social services;
- insurance companies;
- special schools;
- probation and aftercare institutions;
- the Child Care and Protection Board;
- family supervision or guardianship institutions; and
- administrative bodies and benefits agencies that administer certain social security laws.

A separate provision is included in the Wbp concerning the processing of data on hereditary characteristics. Such data may only be processed in respect of the person from whom they were collected. If a person provides an insurer with data on hereditary characteristics about himself for taking out a life insurance, these hereditary characteristics may only be used in connection with that person himself, and not in connection with family members to whom the data necessarily relate as well.

The Wbp requires that the person or body processing personal data is bound by a duty of confidentiality. As far as this duty of confidentiality is not already applicable by virtue of position, profession or a statutory obligation, the Wbp imposes it. Please take into account that not only the Wbp is relevant to the question if you are allowed to process data on someone's health.
Other legislation may also apply, such as for example section 7.5 of book 7 of the Civil Code (on contracts in respect of medical treatment) and the Medical Examinations Act.

7.3.4 General exemptions: remaining provisions

general exemptions

Even if the ban on processing special data cannot be lifted via any of the specific exemptions (for example because you are not one of the controllers that are allowed to process data on health), you may nevertheless be allowed to process such data.

These are the general exemptions. You are allowed to process special personal data if, for example:

explicit consent

- The data subject gave his explicit consent.

Explicit consent means that the data subject must have expressed his will explicitly. This is (even) stronger than the unambiguous consent described in paragraph 3.4.2.

subject made data public

- The data subject has manifestly made the data public himself.

In that case, the intention of the data subject to disclose the data has to be clear. For example, if somebody runs for a political position, he will make public his political points of view. These are special personal data, namely data about someone's political opinions, but under these circumstances you are allowed to process these data.

legal proceedings

- If the processing is necessary for the establishment, exercise or defence of legal claims.

It may occur that you must process certain data about your opponent in legal proceedings, in order to be able to defend your own position.
The ban on the processing of special personal data also does not apply if the processing takes place for purposes of scientific research or statistics, provided that you and your research meet a number of requirements of the Wbp.

Specific forms of data processing

8.1 Direct marketing

8.1.1 What is direct marketing?

To providers of products and services, it is important to maintain a direct relationship with existing customers and to be able to attract new customers. The same is true for charitable institutions with regard to existing and new donors.

direct marketing

The maintenance of a direct relationship with the data subject for commercial or charitable purposes is called direct marketing.

This does not only concern mailings to data subjects, but also the creation of profiles, for example to approach the data subject directly for commercial purposes. You can perform direct marketing in various ways:

- you may approach your customers or donors by using the data from your own customer file;
- you may make use of personal data which another company provides you with, in order to send a message yourself to the people included in that file; and
- you may request another company that has an address file to send a message on your behalf to the people included in that file.

This chapter will deal with the question to what extent you are allowed to use personal data for direct marketing purposes, and what special requirements are set by the Wbp in this respect.

8.1.2 May I perform direct marketing?

general rules

The question whether it is permitted to process personal data for direct marketing purposes must be assessed using the general rules for rightful processing of personal data.

This means, among other things, that the way of processing for direct marketing purposes *may not be incompatible with* the purpose for which you acquired the data (see paragraph 3.5). You always have to take into account the specific circumstances of each case. The extent to which there is a connection between the purpose for which you acquired the data and your concrete direct marketing purpose are of special importance.

- If you acquired the data for a certain direct marketing purpose, further processing for that purpose is of course not incompatible.
- The situation is less clear if you acquired the personal data for another purpose. Often the processing of data for the direct marketing of products or services that are connected to products or services delivered earlier will not be incompatible. This may be otherwise if it concerns completely different products or services than are common in your company or line of business.

- Compatible use is also less likely if the further processing operation consists of your providing the personal data to a third party for direct marketing purposes.

Furthermore, it is important to know *whether a selection is made of the data to be processed and if yes, on what basis this is done.*

If a bank sends information about savings accounts to all clients who have a current account, the processing involved is not incompatible. However, if a health insurance company provides a supplier of protheses with personal data that were selected on the basis of data in the expense claims which the insured person submitted for payment, that way of processing will be incompatible.

Once you ascertained that the intended use of processing for direct marketing purposes is compatible with the purpose for which you acquired the data, you must of course be able to base your processing on one of the grounds described in paragraph 3.4.

Often, direct marketing *is necessary for your legitimate interest in* a sound business administration, and when your interests are balanced against the privacy interest of the data subject, the outcome will often be in your favour. If you have doubts about this outcome, it is advisable to ask the data subject's unambiguous consent to the intended processing operation.

8.1.3 What is objection and what should I do if an objection is raised?

right to object

The Wbp provides that data subjects may complain about the use of their data for direct marketing purposes. Such a complaint is called an objection. This right to object is slightly different from the right to object described in paragraph 4.7.

point out the right to object to the data subject

You must point out to the data subject that he has the right to object:

- If you process data yourself for direct marketing purposes and send direct marketing messages: *in every message* (for example by mentioning an address, telephone number or e-mail address where objections can be sent to).

general announcement

- If you provide personal data which you acquired yourself to a third party for direct marketing purposes, or if you use personal data at the expense of third parties for direct marketing purposes: by means of a *general announcement.*

Examples of a general announcement are, for example, advertisements in daily newspapers or free local papers.

If you regularly provide personal data to a third party, or regularly use personal data for the benefit and at the expense of third parties, you must publish a

general announcement once per year. This announcement can also have the form of an advertisement of a trade association, in which the individual responsibilities are enumerated in a list.

cease immediately

As soon as somebody raises an objection with you against the use of his or her data for direct marketing purposes, you have to cease such use immediately.

However, an objection does not always mean that you will no longer be allowed to use the data of the data subject at all; only the use for direct marketing purposes will no longer be allowed. If, for example, a subscriber to a weekly magazine raises an objection, the publisher can of course continue to use this data subject's data for sending him the magazine and charging him the subscription fee. It will no longer be allowed, however, to send him publicity for other publications.

direct marketing provisions not applicable

The data subject does not have to state a reason for his objection. The objection is free of charge: this means that you are not allowed to charge a fee for the termination of your data processing for direct marketing purposes.

8.1.4 Do the direct marketing provisions of the Wbp apply to any direct contact?

It is widespread practice that communications between supplier and buyer contain a commercial message, although they are not primarily aimed at this message. The direct marketing provisions do not relate to such cases.

This may concern, for example, bank statements on which not only the balance, amounts credited and amounts debited are mentioned, but on which the reader's attention is also drawn to a new way of saving. In this example, communication is not primarily aimed at that commercial message, but the message is of a secondary nature. Another example is the insertion of a leaflet in a newspaper by the newspaper publisher. In such cases, the specific provisions relating to direct marketing are not applicable. This means concretely that if a client opposed the processing of his personal data for direct marketing purposes, you do not have to leave out the message on the bank statement or forego the insertion of the leaflet. In addition, you do not have to point out to the data subject the possibility of raising an objection.

This exception is not applicable in cases where not everyone receives the message or not everyone receives the same message.

If you make a certain selection to determine who will get which message, you must take into account possible objections by data subjects. If you send a message on the basis of a selection, you will also have to point out the possibility to object in that message.

telephone conversation

Another special case is the maintenance of a direct relationship by means of telephone conversations.

If a data subject has objected to the processing of his personal data for direct marketing purposes, you may not telephone that person for those purposes either. On the other hand, you do not have to point out the possibility to object in each commercial conversation you have with a (potential) customer or donor. In such a conversation, the data subject may of course object of his own accord to the use of his data for direct marketing purposes. The trade association of direct marketers (DMSA) has a general telephone line where data subjects can indicate that they do not wish to be approached for direct marketing purposes by telephone.

8.2 Data traffic with foreign countries

8.2.1 Introduction

The globalisation of the economy and the new technical possibilities result in more and more cross-border traffic of data. This opens all kinds of new perspectives, but can also have an advert effect on the privacy of data subjects. The Wbp contains some provisions about the transmission of personal data to foreign countries. In this paragraph, you will learn what these provisions mean for you.

8.2.2 May I transfer data to other countries within the European Union?

data traffic within the EU

The Wbp has no separate provisions about data traffic within the European Union. This is not surprising, since the Wbp was created on the basis of a European Directive. The purpose of that Directive was to allow the free traffic of personal data within the European Union. In order to achieve this goal, a good and high level of protection of personal data had to be created in all Member States. When all Member States will have adapted their legislation, the European Union will have harmonized the law on the protection of personal data.

This means in practice that you may transfer personal data to another Member State without having to meet special requirements. Of course your processing operation must meet, as any national processing operation, the general requirements of the Wbp; see the previous chapters on these. If you meet these requirements, nothing precludes your transfer of data.

If the data transmitted are then processed further by a local branch of your company in that other country, France for example, that further processing operation in France must meet the French rules for privacy.

8.2.3 May I transfer data to countries outside the European Union?

data traffic outside the EU

The Wbp does have some specific provisions on data traffic with countries outside the European Union.

In principle, you may only transfer data to such a country if that country ensures an adequate level of protection.

adequate level of protection

As a controller, you must judge for yourself whether the country in question outside the European Union ensures an adequate level of protection. To this end, you must first examine whether the minister of Justice determined, for example, that a certain country outside the European Union has an adequate level of protection. In that case, transfer will be allowed.

If the minister has not or not yet determined anything, you can go by a judgment of the European Commission on the level of protection in a certain country, if there is such a judgment.

If neither the minister, nor the European Commission gave a judgment, you must examine whether the country to which you want to transfer data offers an adequate level of protection by using the following elements, among others:

- the nature of the data;
- the purpose or purposes of the proposed processing operation;
- the duration of the proposed processing operation;
- the general and sectoral rules of law in force in the country in question; and
- the security measures complied with in that country.

exceptions

If you reach the conclusion that a country does not ensure an adequate level of privacy protection, you may in certain cases still transfer personal data.

This may be the case:

- If the data subject has given his consent unambiguously to the proposed transfer.

This consent must indeed relate to the transfer to the country involved. If you get the data subject's unambiguous consent to the processing of his personal data for direct marketing purposes, this does not yet include a consent to the transfer of those data to a country which does not guarantee an adequate level of protection.

- If the transfer is necessary in connection with a contract between you and the data subject.

If, for example, somebody orders a product with a company in another country, the personal data of the data subject will have to be transferred in order to be able to carry out that order. In that case, no separate, unambiguous consent will be required.

public sector

What is important to the public sector is that a transfer can also take place if:

- the transfer is necessary on important public interest grounds; or
- the transfer is made from a register established by a legal provision that is open to consultation by the public.

An example of the latter is the Commercial Register. The Wbp has some other exemptions from the ban on transfer to a country that does not guarantee an adequate level of privacy protection. Especially since these are exemptions from a ban, you must always carefully examine whether your intended processing operation falls under one of the exemptions.

meeting the requirements of Wbp

We conclude with a general remark: even though you transfer data to foreign countries, this transfer is always a processing subject to the Wbp. Consequently, the transfer must always meet the requirements of the Wbp. This means, among other things, that the transfer may not be incompatible with the purpose for which you collected the data, and that you must be able to base the transfer on one or more grounds provided by the Wbp.

What can happen if I do not meet all requirements of the Wbp?

9.1 Introduction

At the moment you do not comply with the Wbp or the regulations based on it, you may be confronted with various actions:

- A citizen may take steps against you.
- The Public Prosecutions Department may prosecute you.
- The Personal Data Protection Commission may take action.

Anyone who incurs damage by your acting contrary to the Wbp or the regulations based on it may recover this damage from you. Furthermore, the Court may impose an injunction or an order on you. Besides, interested parties may take action against a number of specific decisions taken by you. The Wbp makes a distinction between situations in which you, as a controller, are an administrative body, and situations in which this is not the case.

Violation of certain norms of the Wbp has been qualified as a punishable offence. The Public Prosecutions Department may prosecute you for violation of these norms.

Finally, the Personal Data Protection Commission may take action. The Commission may, among other things, apply administrative coercion or may impose an administrative penalty. These actions will be discussed below. Other possible actions by the Commission, such as conducting investigations into the compliance with the Wbp in a certain sector, are not discussed in this guide.

9.2 What actions may citizens take against me?

9.2.1 General

If you or your branch adopted a code of conduct which includes a regulation for the settlement of disputes, citizens may of course take action on the basis of that regulation. In practice, all kinds of regulations have been adopted for the settlement of disputes. Only the possibilities which citizens have under the Wbp will be discussed below.

9.2.2 Compensation of damage

controller liable

The responsibility to ensure that the Wbp is complied with, and the liability for damage that is the result of non-compliance, rests primarily with you, the controller.

As a controller, you are liable for the damage incurred by anyone as a result of your violation of the Wbp. You will also have to compensate any immaterial damage. In addition, you will be liable if another party, for example the processor called in by you, commits the violation. In that case it may be possible for you to recover the damages paid by you from that processor, but it is you who is liable towards the party incurring the damage. This is only otherwise if you

can prove that you are not responsible for the damage. Under certain circumstances, independent liability rests with the processor. See paragraph 5.3 on this subject.

9.2.3 Injunction or Court Order

injunction or court order

Anyone who incurs damage or is threatened to incur damage as a result of your violation of the Wbp may also ask the Court to impose an injunction or order on you. The Court may, for example, forbid you to provide certain data to a third party, or order you to remove certain data from your system.

9.2.4 I am an administrative body: the interested party may object

decision within the meaning of the General Administrative Law Act

If you are an administrative body, some of your decisions are qualified as decisions within the meaning of the General Administrative Law Act (Algemene wet bestuursrecht). Interested parties may raise an objection against these decisions pursuant to the provisions of this Act. These are always decisions you take at the request of the data subject (or his legal representative). The following decisions are designated in the Wbp:

- the decision on a request for information about the processing operations exempted from the obligation to notify (see paragraph 4.2.3);
- the decision on a request for access to the data (see paragraph 4.4);
- the decision on a request for correction of the data (see paragraph 4.5);
- the decision on a request for notification of the third parties you have informed of a correction (see paragraph 4.5);
- the decision on an objection raised pursuant to Article 41 of the Wbp (see subparagraphs 3.4.6 and 3.4.7);
- the decision on an objection raised pursuant to Article 40 of the Wbp (see subparagraph 8.1.3).

You should be aware that the General Administrative Law Act also applies to the making of these decisions.

9.2.5 I am not an administrative body: the interested party may file a petition

petition

Even if you are not an administrative body, an interested person can take action against the decisions mentioned in the previous subparagraph. In that case, the interested party has to file a *petition* with the Court. An *interested party* is not only the data subject, but may also be, for example, the third party from whom you acquired the data.

The interested party must file the petition:

- Within six weeks after having received your decision.
- If you have not answered within the statutory period (in most cases four weeks), the interested party must file the petition within six weeks after the expiry of that period.

The ordinary petitions procedure of the Code of Civil Procedure (Wetboek van Burgerlijke Rechtsvordering) applies here. In addition to this procedure, the Wbp provides that the Court may offer interested parties the opportunity to express their point of view, if necessary.

9.3 Which violations are punishable offences?

punishable offences

The Wbp attaches punishment to a number of violations of the Act. You may be punished by a financial penalty of NLG 5,000 (€ 2,250) if you, as a controller:

- failed to notify your data processing operation;
- failed to notify your data processing operation fully or correctly;
- do not or do not timely notify any processing operations deviating from your previous notification;
- do not retain processing operations deviating from your previous notification;
- transfer personal data to a country outside the European Union contrary to a prohibition of the Ministry of Justice;
- have not designated a person or institution to act on your behalf if your registered office is neither in the Netherlands, nor in another Member State of the European Union, but you are processing data in the Netherlands by automated or other means.

If you act intentionally when committing any of these summary offences, you can be punished by imprisonment of six months or a financial penalty of NLG 10,000 (€ 4,500).

The Public Prosecutions Department has no right to prosecute you if the Personal Data Protection Commission already imposed an administrative penalty on you for the same offence.

9.4 What actions may the Personal Data Protection Commission take if I do not comply with the Wbp?

9.4.1 Administrative coercion or penal sum

administrative coercion

If you break one or more rules of the Wbp or the regulations based on it, the Personal Data Protection Commission can apply administrative coercion. Administrative coercion consists of granting you a term to remedy your offence. If you fail to do so, the Commission may remedy the offence itself at your expense.

penalty

The Commission may also choose to impose an order on you on pain of a penalty. The Commission will do this if it cannot easily remedy the offence itself. For example, the Commission can order you to remove certain data within one week, or to notify your processing operation within one month, on pain of a penalty for each day on which you fail to comply with this order.

The Commission's decisions are subject to the rules of the General Administrative Law Act. This means, among other things, that the Commission must always grant you a certain period of time to remedy the offence: the so-called begunstigingstermijn (compliance term). It means also that you can object to a decision of the Commission to apply administrative coercion or impose a penalty. The Ministry of Justice published various brochures on the topic of raising an objection.

9.4.2 Administrative penalty

administrative penalty

The Commission may impose an administrative penalty on you in a number of cases. Before the Commission imposes a penalty on you, it must draw up a report. A copy of this report will be sent to you. You are not obliged to make any statements that would incriminate yourself; in other words, you have the right to remain silent. This right arises at the moment you can reasonably suspect that the Commission will impose a penalty on you; for example, at the moment when you receive a copy of the report.

Before imposing a penalty on you, the Commission has to give you the opportunity to express your point of view. If the Commission then decides to fine you nonetheless, you may object to this decision. The Ministry of Justice published various brochures on the topic of raising an objection.

If you can demonstrate that you cannot be blamed for the offence, the Commission cannot impose a penalty on you. The Commission cannot impose a penalty on you either if more than five years have lapsed between the committing of the offence and the imposition of the penalty. If the Commission fines you nonetheless, you must first raise an objection. After the decision on your objection has been given, you have the possibility to start appeal proceedings in Court.

The penalty may not exceed NLG 10,000 (€ 4,500). The Commission has the right to impose this penalty if you, as a processor:

- failed to notify your data processing operation;
- failed to notify your data processing operation fully or correctly;
- do not or not in time notify any processing operations deviating from your previous notification; or
- do not retain processing operations deviating from your previous notification.

You have to pay the penalty within six weeks after the decision has entered into force. The decision to impose a penalty takes effect only when:

- the time to raise an objection has expired; or
- in the event that you raised an objection: at the moment a decision on the objection is given.

If you do not pay in time, the Commission may collect the penalty by means of a Court enforcement order.

From Wpr to Wbp: what has changed and what are the transitional arrangements?

This appendix briefly indicates the most important differences between the old Personal Data Files Act and the new Personal Data Protection Act. The overview given here is not exhaustive. The transitional arrangements are also described.

- *"Processing of personal data"* instead of *"personal data files".*

The Wbp regulates the processing of personal data. This term comprises also the collection, and therefore the acquisition, of personal data. Under the Wpr, this was different. The rules of the Wbp also apply to the collection and acquisition of data.

- *"Controller"* instead of *"holder".*

The Wbp is primarily aimed at the controller instead of the holder. In order to determine who is the controller, the first thing to look at is who has the authority in a formal legal sense to determine the purposes and means of data processing. Only if it is unclear who has this authority, it must be examined to whom the authority can be attributed according to socio-economic standards. Under the Wpr, this was different.

- Distinction between public and private sector was cancelled.

The Wbp is applicable to the processing of personal data without distinction. The duty for the public sector to have regulations was cancelled. Government institutions must also notify their data processing operations with the Personal Data Protection Commission. In such a notification, a lot of information must be provided on the data processing. The norms of the Wbp may be filled in differently in the private and the public sector. This has to do with the different roles of government and private undertakings in society.

- The obligations to provide information were extended.

The controller is obliged to inform the person whose personal data are processed (the data subject) about the processing of the data, unless the data subject is already informed. This was different under the Wpr, where the holder did not have to inform the data subject if the subject *could reasonably be informed.* The Wbp provides a number of other exceptions to this obligation to provide information.

- The data subject has the right to object.

In a number of cases, the data subject has *the right to object in connection with his particular personal circumstances.* The controller has to end the processing operation if such objection is, in his view, justified. If personal data are collected and processed further for direct marketing purposes, the data

subject *has the right to object free of charge.* In the event of such objection, the controller must always end the processing for those purposes.

- Strict liability for unlawful data processing was toned down.

The controller is not liable for damage arising from an unlawful data processing operation if he or she can prove that he or she cannot be blamed for this damage. This regulation is more flexible than under the old Wpr.

- Miscellaneous.

The Wbp partly applies also to the press, radio and television. If personal data are processed for journalistic, artistic or literary purposes, a number of obligations under the Wbp have to be complied with.

The regime for sensitive data (under the Wbp: special data) was somewhat tightened. Special data may only be processed in a concretely defined interest or (further defined) important public interest.

The Wbp introduced the data protection official. The controller or a trade association may appoint such an official.

The powers of the Personal Data Protection Commission (formerly the Registration Chamber) were extended. The Commission may, for example, impose an administrative penalty on you if you fail to notify your processing operations.

Transitional law

Regarding processing operations that were already taking place at the moment the Wbp took effect, you must *within one year* after that moment:

- ensure their conformity with the Wbp; and
- notify them with
  - the Personal Data Protection Commission (formerly the Registration Chamber); or
  - (when appointed) the data protection official.

Please note: You must notify your data processing operations once again under the Wbp, even if you have already notified your registration of personal data under the Wpr. This must be done within one year after the Wbp entered into force. The government may prolong this term to a maximum of three years.

If you begin to process data after the entry into force of the Wbp, your processing operations must meet the provisions of the Wbp at once.

If you process special personal data, you must ensure the conformity of your processing of these special data with the provisions of the Wbp concerning special data within three years after the entry into force of the Wbp. In all other cases, the ordinary transitional arrangements as described below will apply.

If you are processing special data at the time of entry into force of the Wbp on the basis of a contract that was concluded before the entry into force of the Wbp, and this processing operation is necessary to perform that contract, you do not have to request the consent of the data subject anew.

If on the moment of entry into force of the Wbp you are processing data that are subject to a prior check pursuant to the Wbp, you have to notify the Personal Data Protection Commission of this processing operation for such a prior check. You do not have to suspend your processing during the check, however. But if you start such a processing operation after the entry into force of the Wbp, you will have to suspend your processing.

Personal Data Protection Commission (Registration Chamber)
College bescherming persoonsgegevens (Registratiekamer)
Postoffice box 93374
2509 AJ The Hague
fax: 070 381 13 01
e-mail: mail@cbpweb.nl or mail@registratiekamer.nl
website : www.cbpweb.nl or www.registratiekamer.nl

Consultants of the Personal Data Protection Commission: tel. 070 – 381 1300 (from 9.00 to 12.30 h.)

Ministry of Justice
Ministerie van Justitie
Postoffice box 20301
2500 EH The Hague
tel: 070 370 68 50
e-mail: voorlichting@best-dep.minjust.nl
website: www.minjust.nl

VNO-NCW
Postoffice box 93002
2509 AA The Hague
tel: 070 349 03 49
fax: 070 349 03 00
e-mail: informatie@vno-ncw.nl
website: www.vno-ncw.nl/privacy

FNV
Postoffice box 8456
1005 AL Amsterdam
tel: 0900 330 03 00
website: www.fnv.nl

DMSA
Postoffice box 75959
1070 AZ Amsterdam
tel: 020 517 12 12
e-mail: info@dmsa.nl
website: www.dmsa.nl

Association of Dutch Municipalities
Vereniging van Nederlandse Gemeenten (VNG)
Postoffice box 30435
2500 GK The Hague
tel: 070 373 83 93
website: www.vng.nl

Colophon

Publication:
Ministry of Justice
The Hague, April 2001
www.minjust.nl

Editors:
L.B. Sauerwein and
J.J. Linnemann
Kennedy Van der Laan
Amsterdam

T E C T I

O N A C T