

Third countries

CONTENTS

Transfers of Personal Data to Countries
outside the European Union



PERSONAL DATA SHALL BE TRANSFERRED TO A COUNTRY
OUTSIDE THE EUROPEAN UNION ONLY IF THAT COUNTRY CAN
GUARANTEE AN ADEQUATE LEVEL OF PROTECTION



CONTENTS

Foreword	5
1 The transfer of personal data to third countries	6
2 The transfer of personal data to a country where adequate protection exists	9
3 The transfer of personal data on the basis of a statutory exception	13
4 The transfer of personal data under a permit from the Minister of Justice	15
5 Supervision by the CBP	19
Appendices	
- The questions of the Application form for a ministerial permit	21
- Chapter 11 of the Dutch Data Protection Act	24
- Internet addresses	26

FOREWORD

The Dutch Data Protection Act (known by its Dutch initials, WBP), which has been in force since 1 September 2001, contains rules on the transfer of personal data to countries outside the European Union. This is one of the new features of the WBP, and one which is likely to have practical implications for internationally active businesses and other organisations.

The basic rule is that personal data may be transferred to a third country only if the level of protection in that country is adequate. However, a third-country transfer is also allowed if it is covered by a statutory exception, or if a permit has been granted by the Minister of Justice. Ministerial permits are after advice of the Dutch Data Protection Authority (CBP). The CBP also has the job of monitoring compliance with the Act, in connection with which it possesses powers of enforcement.

This booklet is intended to provide general guidance for organisations with an interest in this new field, and for their advisors. References to other useful sources of information are included. Careful and prompt consideration of the relevant issues can ensure that personal data are adequately protected in international transactions, just as they are in the domestic context.

P.J. Hustinx
Chairman



A third country is any country outside the EU, with the exception of other countries in the European Economic Area (EEA) (i.e. Norway, Liechtenstein and Iceland). These three countries have committed themselves to implementing the Directive in their national legislation.

Data traffic within the European Union

The Dutch Data Protection Act (WBP) is based on Directive 95/46/EC of the European Parliament and the Council of the European Union, issued on 24 October 1995 (referred to below simply as ‘the Directive’). The Directive has two purposes: to ensure a uniform level of data protection and to allow the free movement of personal data within the European Union (EU). Once all member states have modified their legislation in line with the Directive, the EU will be a single jurisdiction in the context of data protection. Hence, data traffic between the Netherlands and another EU country will only have to meet the general requirements of the WBP.

[< PREVIOUS](#)

[CONTENTS](#)

[NEXT >](#)

Third countries

In view of the increasing technical scope for large-scale data exchange and the internationalisation of business, the legislator felt it necessary to devote a separate chapter of the WBP (chapter 11, articles 76-78) to data traffic between the EU and third countries.

The basic implication of chapter 11 of the WBP is that personal data can be transferred to a third country only if the general requirements of the WBP are met and if the third country in question guarantees an adequate level of protection. One of the general requirements is e.g. that the processing is notified to the Dutch Data Protection Authority (CBP). This booklet deals only with those conditions that relate to the transfer of personal data from an EU country to a third country.

What is a transfer?

An act by which personal data are made available to a party located outside the legal jurisdiction of an EU country constitutes the transfer of personal data. To fall within the legal definition, such an act must be performed knowingly, with the purpose of conveying the data in question beyond EU territory to a third country. Here are a few examples of situations that involve data transfer:

- A company in an EU country sends personal data by e-mail to a company outside the EU in the context of a direct marketing campaign.
- An internationally active concern maintains a database in one of the countries in which it has a presence. This database contains information about the concern's entire international workforce. All the concern's subsidiaries inside and outside the EU are able to download data from and upload data to the database.
- A company in an EU country is taken over by a company from outside the EU.

The three circumstances under which transfers may take place

The WBP defines three circumstances under which personal data may lawfully be transferred from the EU to a third country. First, personal data may be transferred as long as the third country in question provides an adequate level of protection. If the third country does not provide adequate protection, a transfer may nevertheless be made, if one of the exceptions described in the WBP applies.

Finally, in cases where none of the statutory exceptions apply, it is possible to obtain a transfer permit from the Minister of Justice. Someone who wishes to transfer personal data to a third country should therefore decide (on the basis of the situation in that country) which of the circumstances referred to above applies, and then proceed accordingly. The three grounds for lawful transfer do not have any order of priority. The European Commission (EC) and the EU member states have a common policy, under which certain third countries are regarded as offering an adequate or partially adequate level of protection.

This booklet is intended to provide general guidance for organisations with an interest in this field. For further information, please refer to the *Policy paper on transfers of personal data to third countries in the context of the new Dutch Data Protection Act (WBP)*, which is posted on the CBP web site (www.cbpweb.nl).



2

→ THE TRANSFER OF PERSONAL DATA TO A COUNTRY WHERE ADEQUATE PROTECTION EXISTS

To determine whether a country provides an adequate level of protection, the data controller should first establish whether either the Minister of Justice or the EC has passed a ruling concerning the level of protection in the country concerned. You are the data controller if you are the party who determines the object and means of processing and if the personal data is used in your interest. In this context, data processing means any procedure involving data, from the collection of data to the destruction of data. Transfer is therefore a form of data processing.

If neither the Minister nor the EC have made a ruling regarding the country, you must make an assessment yourself by reference to certain criteria. The criteria specified in the Directive and the WBP relate to the nature of the data, the purpose and duration of the proposed processing, the country of origin the ultimate destination country, and the statutory rules, appeals codes and enforcement system in the country in question. The Minister of Justice provided information regarding the criteria to the Lower House of the Dutch parliament in a letter dated 9 March 2000.

Guidelines on the application of the criteria have also been developed by a working party made up of representatives from the national supervisory authorities (known as the Article 29 Working Party), set up in accordance with the Directive.

What constitutes an adequate protection level?

Before the Directive came into effect, the Article 29 Working Party of its own accord issued a document dealing with the concept of an adequate protection level. This document sets out a number of principles that the system of protection in a country should incorporate in order to be considered adequate. These principles form important practical guidelines for use when assessing the level of protection afforded by a country. The working party advises basing assessment both on the nature of the applicable legal provisions and on the means by which they are enforced.

To be considered adequate, the data protection provisions in a country should incorporate the following principles:

Purpose limitation Personal data processing should always be processed for a specific purpose and personal data should only be used or further communicated if this is not incompatible with the purpose of the transfer.

Quality and proportionality Personal data should be accurate and up to date. The data should also be adequate and relevant in relation to the purpose of the transfer.

Transparency The people to whom the data relate (the data subjects) should be provided with information regarding the purpose of the data processing and the identity of the data controller in the third country. Any other information necessary to ensure fairness should be provided.

Security The data controller should take technical and organisational security measures that are appropriate to the risks presented by the processing. Anyone acting under the authority of the data controller may process personal data only in accordance with the latter's instructions.

Rights of the data subject An individual should have a right of access to data concerning him or her. The individual should also be able to have incorrect data corrected. Under certain circumstances, an individual should also be able to object to the processing of data concerning him or her.

The requirements made by the Working Party with regard to the enforcement situation in the third country are as follows:

Adequate level of compliance A number of factors are relevant in this context. First, private individuals and data controllers should be aware of their rights and obligations. There should also be scope for the application of effective sanctions against those who fail to respect the data protection principles. Finally, the supervisory authority, auditors or other authorities should have adequate powers to monitor compliance.

Availability of assistance Assistance should be available to individuals to enable them to exercise their rights.

A mechanism must exist, by which an individual is able to exercise his or her rights quickly, effectively and without incurring unreasonable expense.

Appropriate redress If an individual's interests are harmed as a result of someone failing to respect the data protection principles, he or she should be able to obtain proper redress (compensation).

The Working Party's guidelines relate to the assessment of the general level of protection in a country. However, someone who is considering the transfer of personal data must assess the adequacy of the protection afforded in the specific circumstances of the proposed transfer. In some cases, it may be necessary to ascertain that additional protection is provided; in others, a lower level of protection may suffice.

Suppose, for example, that you wish to exchange medical data with a party in a third country for research purposes. You should find out whether the country in question has adequate legislation regarding the protection of medical data and that there are sufficient assurances that such data will be treated with proper care. The *Policy paper on transfers of personal data to third countries in the context of the new Dutch Data Protection Act (WBP)* contains a checklist, which you can use to help you decide whether a country provides an adequate level of protection. However, it is your responsibility to assess the level of protection that exists in a country; the CBP can only offer general guidance. More information about the guidelines issued by the Working Party is given in the policy paper and on the EC web site.

European Commission rulings on the adequacy of protection

The EC makes rulings on the adequacy of protection in particular countries and in relation to particular economic sectors. These rulings are binding on all EU member states. If the EC has not made a ruling regarding the protection level in a given country, it does not follow that the country in question does not provide an adequate level of protection for the transfer of personal data. The EC has so far issued positive rulings concerning Switzerland, Hungary, part of Canada and a number of businesses in the United States that have agreed to abide by the so-called “Safe Harbour Principles”.

If you are unsure about the adequacy of the protection that exists in a given country, the CBP recommends that you take no unnecessary risks. Establish whether the data transfer you are contemplating is covered by one of the statutory exceptions, or consider applying for permission from the Minister of Justice.



3

→ THE TRANSFER OF PERSONAL DATA ON THE BASIS OF A STATUTORY EXCEPTION

If a third country does not provide adequate protection, it may nevertheless be possible to transfer personal data to that country. A transfer is lawful under such circumstances either if you obtain a ministerial permit (see article 4), or if the situation is covered by one of the exceptions defined in the WBP. Remember, though, that the general requirements of the WBP must also be complied with in all cases.

The exceptions defined in the WBP are as follows:

- The data subject has given his or her unambiguous consent. The data subject is the person to whom the data to be processed relate. You must inform the data subject about the level of data protection in the country to which the data is to be transferred. If the data subject has been informed of your intention and has not objected, this is not sufficient to make the transfer lawful – the data subject must actually consent;

- The transfer is necessary for the fulfilment of a contract between you and the data subject. In the context of a contract, it is sometimes necessary to make personal data concerning the subject available to a third party. This might be the case when reserving an airline ticket, for example, or when making an international payment via a bank or using a credit card;
- The transfer is necessary for the fulfilment of a contract to which the data subject is not a party, but in which he or she has an interest. If someone closes an insurance contract in the Netherlands, for instance, the insurer may need to obtain re-insurance abroad. In this context, personal data concerning the insured might have to be sent to a third country. This exception does not cover transfers made for direct marketing purposes, since such a transfer is not in the interest of the data subject;
- The transfer is necessary on important public interest grounds, or for the establishment, exercise or defence in law of any right. If, for example, personal data is transferred to a debt collection agency in a third country to enable the agency to take legal action, this exception applies;
- The transfer is necessary for the protection of the vital interest of the data subject. If someone has an accident or falls ill abroad, it may be necessary to send that person's medical records to a hospital in a third country without waiting for consent or clearance, for instance;
- The transfer is made from a public register set up by law that is open to general consultation (e.g. a trade register or land register).



4

→ THE TRANSFER OF PERSONAL DATA UNDER A PERMIT FROM THE MINISTER OF JUSTICE

If it is not possible or desirable to rely on any of the statutory exceptions to justify a transfer to a third country where protection is not adequate, consideration may be given to obtaining a permit from the Minister of Justice. If a permit is granted, the Minister may attach conditions in order to protect the privacy or the fundamental rights and freedoms of the data subject(s). These conditions may, for example, relate to the contractual clauses with the party to whom the data is to be transferred, including certain provisions. The CBP advises the Minister of Justice regarding the issue of permits.

Use of a model contract expedites permit procedure

One way of ensuring that adequate safeguards are provided is to use one of the model contracts approved by the EC. The EC has a approved model contract covering transfers between two controllers, one inside the EU and the other outside, and has approved a contract covering transfers to processors in a third country. The use of a model contract expedites the permit procedure.

Adequate safeguards must be provided

The use of a model contract approved by the EC can help you to obtain a permit from the Minister of Justice. However, it is also possible to obtain a permit by making other contractual provisions that have the same effect as those approved by the EC – in other words, provisions that adduce adequate safeguards. When assessing a permit application, the CBP applies the criteria laid down by the Article 29 Working Party (see chapter 2). The application of these criteria is adapted to the specific circumstances of the case.

Contractual provisions should first specify the data recipient's obligations and how these obligations are to be fulfilled. With a view to providing clarity for the data subject, the contract should also make provisions for supervision and for sanctions to be taken in the event of default.

To a large extent, the amount of freedom that the third-country recipient has with regard to the processing of the data determines the risk associated with the transfer. If the responsibility for data processing in a third country lies with a company based in an EU country, the privacy legislation of the EU country in question applies to the processing. Hence, the risk to the data subject is limited, since an aggrieved subject can complain to the controller and the supervisory authority in the relevant EU country. The risk is greater if a controller in an EU country transfers data to a controller in a third country, since EU law ceases to apply once the transfer has taken place. Under such circumstances, it is therefore necessary to make contractual provisions to protect the rights of the data subjects.

The contractual provisions should also address the reliability and liability of the parties to the contract. It must be stipulated, for example, that a data subject can obtain redress from the EU-based controller in the event of an infringement of the subject's rights.

Contractual provisions are particularly useful for the regulation of similar repetitive transfers. The transfers typically made by large international networks, such as credit card transaction networks and airline ticket reservation networks, come under this heading.

Relationship between the European Commission and EU member states

The authorities in an EU member state are obliged to recognise the use of a model contract approved by the EC. However, the supervisory authorities in the individual member states remain responsible for monitoring compliance with the provisions of privacy legislation. Once it has been decided at EU level that a third country provides adequate protection generally or in relation to certain categories of transfer, a member state cannot prevent or restrict data traffic on the basis of its own assessment of the situation in that third country.

Procedure for obtaining a permit

If you wish to obtain a ministerial permit, you should apply to the CBP directly, using the special form apply to the CBP, using the special form posted on the CBP web site.

The CBP divides applications into three categories:

- 1 The applicant proposes to use an EC model contract without addition or amendment. In this case, the CBP simply determines that the contract is correct, complete and not inconsistent with the WBP, then forwards the application and accompanying documentation to the Minister with a recommendation regarding acceptance/rejection.
- 2 The applicant proposes to use an EC model contract, with additions. In this case, the CBP will only recommend acceptance of the application if the additional provisions are not in conflict with the model contract's standard provisions and/or with the rights of the data subjects. If the CBP concludes that there is a conflict, the applicant is given the opportunity to revise the provisions concerned within a specified period.
- 3 The applicant proposes to use an amended version of an EC model contract, or to use a non-approved contract. The model contracts stipulate that their text should be used unamended. Nevertheless, parties seeking to contractually regulate a transfer may devise provisions of their own that relate to the particular circumstances of the transfer. If an applicant chooses to take this course, the CBP has to carefully examine the provisions, and is no longer bound to recognise the contract as adducing adequate safeguards. The CBP will inform the applicant how long it will take to make a recommendation.

If the Minister, after consulting the CBP, decides that a permit should be issued, the Minister is obliged to inform both the EC and the other EU countries of the decision.

Furthermore, permits do not have retrospective effect. In other words, a permit cannot legitimise a transfer that has already taken place or is already in progress; transfers made prior to the date that a permit takes effect are unlawful, unless they were based on another ground.

A controller whose permit application is rejected may appeal against the decision.

Obligatory notification

The duty of notification is also applicable in the case of personal data transfers, regardless of whether those are made to a third country with an adequate level of protection or to a company that has signed up to the Safe Harbour Principles, and those made under a ministerial permit.



5

→ SUPERVISION BY THE CBP

If a country does not provide an adequate level of protection, any transfer to that country is unlawful unless covered by a statutory exception or a ministerial permit. If a transfer is unlawful, it should be terminated immediately and, if possible, the consequences should be negated.

In its supervision activities, the CBP focuses primarily on categories of transfer that entail special risks, such as:

- Transfers involving sensitive data (in the sense of the WBP);
- Transfers that involve a financial risk, such as credit card transactions via the Internet;
- Transfers that involve a threat to personal safety;
- Transfers in connection with decisions that are of great importance to the data subject, such as decisions concerning recruitment, selection, promotion and credit provision;
- Transfers that could be damaging to the honour and reputation of the data subject;
- Repetitive transfers of bulk data, such as electronic data processed via the Internet;

- Transfers involving encrypted or secret bodies of data, such as “Internet cookies” or electronic calling cards.

The General Administrative Law Act allows the CBP to order a controller to comply with the law on data protection or to impose a penalty for failure to do so. If investigations reveal that a third country does not provide adequate protection, the CBP has to inform the Minister of Justice. The Minister may then inform the EC. A ministerial permit may be revoked or its conditions modified if the EC decides, on the basis of new information, that the level of protection in the third country concerned is not adequate or no longer adequate.

The CBP monitors compliance with the WBP by controllers based in the Netherlands who transfer data to third countries. Investigations into the activities of such controllers are often, but not always, made in response to complaints received from members of the public.

APPENDIX: THE QUESTIONS OF THE APPLICATION FORM FOR A MINISTERIAL PERMIT

To apply for a permit, you must use the special CBP application form. This form is posted on the CBP web site: www.cbpweb.nl.

The questions on the form are as follows:

Data concerning the parties involved in the transfer

Data exporter

Data exporter is (please specify briefly your activities relevant to the transfer) established in country (please specify).

Data importer

Data importer is (please specify briefly your activities relevant to the transfer) established in country (please specify).

Data subjects

The personal data transferred concern the following categories of data subjects (please specify). Where appropriate a distinction should be made according to the different types of data.

Purposes of the transfer

The transfer is necessary for the following purposes (please specify). Where appropriate a distinction should be made according to the different types of data.

Categories of data

The personal data transferred fall within the following categories of data (please specify).

Sensitive data (if appropriate)

The personal data transferred fall within the following categories of sensitive data (please specify).

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients (please specify). Where appropriate a distinction should be made according to the different types of data.

Storage limit

The personal data transferred may be stored for no more than (please indicate). Where appropriate a distinction should be made according to the different types of data.

Contact-person

Please indicate the name and contact-details of a contact-person for the exporter and the importer for further communication with the Dutch Data Protection Authority

Basis for the permit

Which instrument has been used by the parties in order to adduce “adequate safeguards” for the intended data transfer? (Please indicate. A copy of the relevant parts of the instrument should be sent together with this form.)

Have you made use of the model contracts approved by the European Commission? Yes No

If your answer to the previous question was positive please answer the following additional questions.

- Please indicate the complete reference of the European Commission model contract you have used.
- Have you added any provisions to the existing model contract?
Yes No If so, please indicate which ones
- Have you amended any of the provisions of the standard contract?
Yes No If so, please indicate which ones.
- Have you used any other existing contract non-approved by the European Commission such as the ones of ICC, CBI, Council of Europe 1992?
Yes No If so, please specify which one.
- Have you, or your affiliates, demanded authorisation in other EU Member States for a similar transfer on the basis of the same or a similar instrument?
Yes No If so, please specify in which Member State(s).

Please indicate any additional information you would like to communicate regarding this transfer.

Signature

The completed form has to be signed (name and authorised signature) by the Data exporter. The exporter declares also that all relevant documentation for the evaluation of the adequacy of the safeguards is sent to the CBP together with this form.

APPENDIX: CHAPTER 11 OF THE DUTCH DATA PROTECTION ACT

Chapter 11.

Data transfer to countries outside the European Union

Article 76

- 1 Personal data that are subject to processing or intended for processing after their transfer shall be transferred to a country outside the European Union only if, without prejudice to compliance with the provisions of this Act, that country guarantees an to compliance with the provisions of this Act, that country guarantees an adequate level of protection.
- 2 The adequacy of the protection level shall be assessed on the basis of the circumstances affecting a personal data transfer or category of transfers. In particular, consideration shall be given to the nature of the data to be transferred, the purpose(s) and duration of the proposed processing operation(s), the country of origin and the ultimate destination country, the general and sector-specific legal provisions that apply in the third country concerned, as well as to the professional rules of conduct and the security provisions applied in this country.

Article 77

- 1 By way of derogation from article 76, a personal data transfer or a category of such transfers may be made to a third country that does not guarantee an adequate level of protection provided that:
 - a the data subject has given his unambiguous consent;
 - b the transfer is necessary for the performance of a contract between the data subject and the data controller, or for implementation at the data subject's request of pre-contractual measures necessary for the conclusion of a contract;
 - c the transfer is necessary for the conclusion or performance of a contract in the data subject's interest between the data processor and a third party;
 - d the transfer is necessary on important public interest grounds, or for the establishment, exercise or defence in law of any right;
 - e the transfer is necessary for the protection of a vital interest of the data subject, or

- f the transfer is made from a public register set up by law that may be freely consulted by anyone or by anyone who can demonstrate a legitimate interest, insofar as the statutory conditions for consultation are met in the particular case.
- 2 By way of derogation from the provisions of subsection 1, Our Minister may, having obtained the advice of the Data Protection Authority, issue a permit for a personal data transfer or a category of such transfers to a third country that does not guarantee an adequate level of protection. Such conditions shall be attached to this permit as are necessary to protect personal privacy and personal fundamental rights and freedoms, and to guarantee the exercise of the associated rights.

Article 78

- 1 Our Minister shall inform the Commission of the European Communities of:
 - a the cases in which, in his opinion, a third country does not guarantee an adequate level of protection in the sense of Article 76, paragraph 1, and
 - b a permit issued pursuant to Article 77, paragraph 2.
- 2 Where a corresponding ruling has been made by the Commission of the European Communities or by the Council of the European Union, Our Minister shall issue a ministerial decree or order to the effect that:
 - a the transfer of personal data to a country outside the European Union is prohibited;
 - b a country outside the union is considered to guarantee an adequate level of protection, or
 - c. a permit issued pursuant to Article 77, paragraph 2, is revoked or revised.
- 3 A notice as referred to in paragraph 1, letter a or b, shall be published in the Staatscourant (Dutch official Journal).

APPENDIX: INTERNET ADDRESSES

- The *Policy paper on transfers of personal data to third countries in the context of the new Dutch Data Protection Act (WBP)*, D. Alonso-Blas (College bescherming persoonsgegevens 2002), is posted on: www.cbpweb.nl
- The letter from the Minister of Justice to the Lower House dated 9 March 2000 (Proceedings of the Lower House, parliamentary year 1999-2000, 27 043, no. 1) is posted on: www.overheid.nl
- The recommendations of the Article 29 Working Party regarding assessment of the adequacy of protection (Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. WP 12.) are posted on: www.europa.eu.int/comm/privacy
- On the same site you can find information about model contracts and the European Commission's rulings regarding the protection levels in third countries.



COLLEGE BESCHERMING PERSOONSgegevens

The Dutch Data Protection Authority (CBP) was created by the Dutch Data Protection Act (WBP). Its job is to supervise compliance with the laws governing the use of personal data. All activities involving the use of personal data must be notified to the CBP, unless covered by a dispensation.

Advice, mediation, investigation and intervention

The CBP advises the government and other organisations regarding data protection and related matters. The CBP assesses codes of conduct and mediates in disputes between members of the public and the users of personal data. On its own initiative or at the request of an interested party, the CBP may investigate the way in which personal data are used in a particular situation, with a view to establishing whether such use is lawful and taking action to prevent unlawful use. A penalty may be imposed on anyone who fails to notify the use of personal data. The CBP can also issue an order against or impose a penalty on anyone who uses personal data in an unlawful way.

The CBP publishes an annual report regarding its activities and rulings. The CBP must exercise its authority in accordance with the standards laid down in the General Administrative Law Act. Objection or appeal may be made against a decision of the CBP. Furthermore, the conduct of the CBP may be investigated by the National ombudsman.

Information

For more information, visit the CBP's web site: www.cbpweb.nl. All CBP publications can be ordered via or downloaded from the website; orders may also be placed by phone. For preliminary advice, you can contact the CBP by telephone on mon-tue-thu-fri between 9am and 12.00 pm. The number to call is +31 (0)70 381 1300.

No rights may be derived from the content of this booklet.

COLOPHON

September 2002

Published by: Dutch Data Protection Authority

Text: S.M. Artz

Design: Proforma, strategie, ontwerp
en management, Rotterdam (Miriam Monster)

Print: Sdu Grafisch Bedrijf, Den Haag

DATA PROTECTION AUTHORITY

Prins Clauslaan 20

Postbus 93374

2509 AJ Den Haag

TEL +31 (0)70 381 13 00

FAX +31 (0)70 381 13 01

E-MAIL info@cbpweb.nl

INTERNET www.cbpweb.nl

< PREVIOUS

CONTENTS

NEXT >