DATA PROTECTION ASPECTS WITHIN THE FRAMEWORK OF SOCIO-ECONOMIC RESEARCH

Other titles from the RESPECT Project:

An EU Code of Ethics for Socio-Economic Research
Dench S, Iphofen R, Huws U
IES Report 412, 2004. ISBN 1 85184 342 6

Intellectual Property Aspects of Socio-Economic Research
Gnädig N, Grosse Ruse H, Giannakoulis M
IES Report 413, 2004. ISBN 1 85184 343 4

Functional Map of a European Socio-Economic Research Project
Schryvers E, Van Gyes G, Vanderbrande T
IES Report 414, 2004. ISBN 1 85184 344 2

Socio-Economic Research in the Information Society:
A User's Guide from the RESPECT Project
Huws U
IES Report 416, 2004. ISBN 1 85184 346 9

A catalogue of these and over 100 other titles is available from IES, or on the IES Website, www.employment-studies.co.uk

For online resources, see www.respectproject.org

r e s p e c t project

professional and ethical codes for socio-economic research in the information society

Data Protection Aspects Within the Framework of Socio-Economic Research

Karen Rosier
Isabelle Vereecken

Under the supervision of
Prof. Dr Yves Poullet
Dr Cécile de Terwangne

CRID
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT

a project funded by the European Commission's Information Society Technologies (IST) Programme

ies
institute for employment studies

Published as IES Report 415 by:

THE INSTITUTE FOR EMPLOYMENT STUDIES
Mantell Building
Falmer
Brighton BN1 9RF
UK

Tel. + 44 (0) 1273 686751
Fax + 44 (0) 1273 690430

www.employment-studies.co.uk

Centre de **R**echerches **I**nformatique et **D**roit
Rempart de la Vierge, 5
5000 Namur

Tel. + 32 81 72 47 69
Fax + 32 81 72 52 02

www.crid.be

British Library Cataloguing-in-Publication Data

A catalogue record for this publication is available from the British Library

ISBN 1 85184 345 0

Printed in Great Britain

The RESPECT project is about:

RESPECT for research ethics

RESPECT for intellectual property

RESPECT for confidentiality

RESPECT for professional qualifications

RESPECT for professional standards

RESPECT for research users

The aims of the project are to:

- develop a voluntary code of practice for the conduct of socio-economic research in the information society
- contribute to the development of common European standards and benchmarks for socio-economic research
- contribute to the development of high standards in cross-national and cross-disciplinary socio-economic research
- contribute to broader ethical and professional debates within the socio-economic research community
- help reduce barriers to the mobility of socio-economic researchers within the EU and Accession States
- provide succinct information on good practice in socio-economic research for research users both inside and outside the IST community.

For full details, see the project website: **www.respectproject.org**

Acknowledgements

We would like to thank Maria-Veronica Perez-Asinari, Jan Dhont and Séverine Dussolier (CRID fellows), Natascha Gnänig and Katrin Knorpp (ITM) for their help in this work.

Contents

Executive Summary

- When drafting these guidelines, the authors had to take into consideration the fact that data protection is regulated by law and that, beyond the general recommendations that can be given to the researchers, the latter are obliged to comply with the relevant applicable law(s).
- This document has been drafted taking into account Directive 95/46/CE and the national legislation of most of the current Member States of the European Union (the Member States) that implement it (the national legislations).
- These guidelines do not include a review of the existing legislation regarding the processing and disclosure of company-specific data, such as trade secrets, that might be protected by law. After examination of the possibility to extend the scope of these guidelines to such kinds of data, the RESPECT partners concluded that this was not feasible in the framework of this project.
- This document does not provide an exhaustive description of the legal regimes in force in all Member States. Indeed, only the English version of the national laws in force and available (at the beginning of 2003) have been taken into consideration. It is possible that recent modifications and/or secondary legislation have not (yet) been translated and published.
- The present guidelines do not detail the existing legislation, other than the data protection statutes. Nevertheless, other legal sources can also be relevant when processing personal data in the framework of research projects. For instance, the present guidelines do not detail the Member States' laws regarding processing of data provided by national institutes of statistics, or the laws implementing Directives 97/66/CE and 2002/58/CE regarding data protection in the telecommunication and electronic communication fields.
- Given the existing divergences between national laws, the authors, with the agreement of the other RESPECT partners, have decided to devise these guidelines as a tool that can be used by researchers to better understand EU data protection legislation.
- For reasons of briefness and simplification, these guidelines cannot help with accuracy for each concrete situation. Therefore, they cannot replace the advice of national experts.

Guidelines on Data Protection Issues Relating to European Socio-Economic Research

Socio-economic research involves the collection and other further processing of personal data. The processing of personal data is regulated by law, and the researchers have therefore to comply with these legal requirements.

These guidelines have been drafted taking into account Directive 95/46/CE and the national legislation of most of the current Member States of the European Union that implement it. They outline the general principles governing data protection, provide for key concept descriptions, and include a series of recommendations, allowing the researcher to take into consideration the various requirements in the field of data protection.

Socio-economic research with respect to data protection requirements encompasses the following principles:

- Draft an outline of the processing operations involved in order to assess the legality of the envisaged processing prior to starting the processing.
- Respect the conditions regarding the selection and use of the data.
- Respect the conditions regarding the legitimacy of the processing.
- Comply with the information duty towards data subjects.
- Comply with duties towards national data protection authorities.
- Respect the rights of the data subjects.
- Take technical and organisational measures to ensure the security and confidentiality of personal data.
- Comply with requirements regarding the re-use of personal data for purposes other than the initial purposes of collection.
- Comply with the conditions for communication of personal data to third parties or recipients.
- Comply with the conditions for the transfer of personal data to countries outside of the European Economic Area.

1. Introduction

1.1 Scope of the guidelines

The purpose of the present report is to provide guidelines to socio-economic researchers conducting research in the European Union regarding the processing of personal data for the purpose of their research projects.

These guidelines are therefore relevant for the processing of personal data carried out strictly for *scientific* and *statistical* purposes (the term purpose is defined in section 1.3.7 and the terms statistical or scientific purposed are defined in the Glossary) **in the field of socio-economic research by a researcher**, whether a legal or a natural person, a private or a public person.

For the purpose of these guidelines, the term 'socio-economic research' will refer to the concept as defined in the Glossary. **It excludes any research project carried out for commercial, marketing, or medical purposes.**

The researcher will have to ensure that the planned processing of data to be carried out is compliant with the relevant law(s) applicable to the processing. Indeed, even when the researcher is not the person legally liable for data protection issues, they need to be aware of these legal requirements and recommendations, because it will often be them who actually conducts the research.

Given the importance of the existing differences between the national legal regimes, the present document only provides general common principles that have to be kept in mind when processing personal data. Some national divergences are explored, but these cannot be considered exhaustive. Readers will still have to refer to the relevant national laws or codes of conduct that have been approved by national data protection authorities, and the defined guidelines that have been designed specifically in reference to the law of that particular country.

1.2 Key principles

The key principles relevant to the processing of personal data were first established by the Council of Europe,[1] and further implemented in the Directive 95/46/CE of the European Union.

The purpose of the Directive is to allow the free flow of personal data between Member States. The other objective of the Directive is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

The protection granted by the Directive does, however, go further than the protection of the *intimacy* of the natural persons *ie* generally speaking their private life, and more particularly, any sensitive data such as that relating to their religion, health, political opinions, *etc.* It deals with the protection of *all the data related to natural persons* and not necessarily only the sensitive data. Therefore, the Directive also applies to data related to natural persons in the context of their professional life (such as their function, telephone number at work, *etc.*).

The Directive defines specific conditions and restrictions guaranteeing the protection of data subjects, but the Member States are not allowed to restrict or prohibit these flows to a greater extent than permitted in the framework of the Directive. A specific regime regarding the transfer of personal data to non-EEA countries has been put in place to protect the data subjects whose data are exported outside the territorial scope of the application of the Directive.

1.3 Key concepts

1.3.1 Personal data

According to Article 2.a of the Directive, the term 'personal data' refers to '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*'. To be considered as personal data, the data:

[1] The Convention no. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data and Recommendation R(97) 18 of the Committee of ministers of Members States concerning the protection of personal data collected and processed for statistical purposes. This latest recommendation concerns more specifically the processing for statistical purposes, whereas the Recommendation of 1983 it replaced concerned both processing of scientific and statistical purposes.

- might concern any information regarding the data subjects such as their name, their email address, an opinion, a sound or an image, or their personal circumstances, whether these relate to the data subject's private, professional or public life. The data might directly concern the data subjects (*ie* specific information about a person) or indirectly concern a person (for example, where the information concerns in the first instance a production process, but indirectly provides information regarding the performance of the persons participating in the production process).
- must relate to natural persons. Data strictly relating to companies, public bodies, *etc.* are not personal data.[1]
- might concern persons that are alive or dead at the moment of the processing.[2]
- must allow the direct or indirect identification of the data subject. In most of the Member States, the possibility of identifying a person through the data is assessed *in abstracto*; the mere existence of a possibility to establish a link between the data and a person being sufficient. [3] Therefore, the fact that data are not directly related to a person does not necessarily imply that they do not constitute personal data.
    - Data allowing *direct identification* are data that can be easily related to a data subject and reveal their identity. This is the case of data such as the name, address, date of birth or even genetic data which, when combined with one another, allow identification with a small margin of doubt. Moreover, a person may be considered as being identified without necessarily knowing the name or address of the person: an IP address may be considered as personal data[4] if it is used to profile the user of the IP address.
    - Indirect identification requires further steps to make a link between a specific person and the data being processed. For instance, in the field of socio-economic research, this indirect link between a person and their data may result from the fact that the sample of the study is very narrow, or that the data collected about a data subject are specific

---

[1] However, in some countries, the data related to companies are protected as personal data.

[2] However, in some of the Member States, personal data only concern alive persons.

[3] In some other States, such as the United Kingdom, or under Irish, Austrian and Dutch law, this assessment is made *in concreto, ie* while taking into account the information which is, or is likely to be, in the possession of the controller, to identify the data subject through the data.

[4] See, for example, the working document of 21 November 2001 of the Group 29 on Privacy on the Internet – An Integrated EU Approach to Online Data Protection, p.17, about profiling of Internet users.

enough to allow a linkage between the data with the person concerned.[1]

- Coded or pseudonymous data, *ie* data in which the identifiers have been reversibly coded,[2] are to be considered as personal data.[3]

However, the concept of 'personal data' does deviate from this definition in certain Member States' national law.

See exceptions and particularities under national laws (Grid 1).

1.3.2 Data subject

The data subject is generally defined as the person to whom the personal data relate.

1.3.3 Anonymous data

There is no specific definition provided for this term in the Directive.[4] For the purpose of the present guidelines, anonymous data will be defined as data that cannot be qualified as personal data, since they do not (anymore) allow direct or indirect identification of the data subject. The processing of anonymous data is not subject to the legal data protection requirements. However, the processing carried out to render data anonymous is considered to be the same as processing personal data. To escape the legal requirements arising out of the processing of personal data, the processed data must already be anonymised. Until the moment the data are rendered anonymous, the controller must comply with all the legal requirements for the processing of personal data.

---

1 Sources: '*Privacy bij wetenschapplijk onderzoek en statistiek. Kadre voor een gedragscode*', College Bescherming persoonsgegevens, May 2002; UK's legal guidance regarding the Data Protection Act 1998.

2 Definition provided in the Belgian Royal Decree.

3 The solution may differ in a country which has an *in concreto* approach according to which the coded data does not qualify as personal data to a controller who does not have the code key.

4 According to Italian law, anonymous data is data '*which by origin, or by its having processed, cannot be associated with any identified or identifiable data subject*'. According to German legislation, '*Rendering anonymous' means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual*.' The Spanish Data Protection Act contains a definition on the process to turn personal data into anonymous data: '*Dissociation procedure: any processing of personal data carried out in such a way that the information obtained cannot be associated with an identified or identifiable person.*'

1.3.4 Sensitive data

This term, used in the Directive, refers to specific categories of data revealing sensitive information about a data subject. The information does not need to directly translate sensitive information, it suffices that it indirectly implies or induces sensitive information to qualify as sensitive data.

For instance, the religious belief of a person is considered to be a sensitive data: the information Mr L. is Muslim is a sensitive data and the information Mr L. fasts for Ramadan is also considered as sensitive to the extent that one can infer that Mr L. is Muslim.

The data considered as being sensitive may be categorised as follows:

- data revealing racial or ethnic origin
- data revealing political opinions, religious or philosophical beliefs
- data revealing trade union membership
- data concerning health (including mental health) or sex life
- data relating to offences, criminal convictions or security measures, and data relating to administrative sanctions or judgements in civil cases
- other categories of sensitive data.

However, the definition may differ in some Member States.[1]

See exceptions and particularities under national laws (Grid 2).

When these guidelines refer to sensitive data in the context of the application of a national law, it is understood that the term 'sensitive data' refers to data that are considered to be sensitive under this particular law.

1.3.5 Processing

The concept of processing is very broad. It concerns any operation or set of operations that are performed upon personal data, whether or not by automatic means. Data processing is considered to be the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available (*eg* by allowing the inspection of data retrieval by a third party), alignment or combination, blocking, erasure or destruction of personal data.

The application of data protection legislation is limited to automated processing and to non-automated processing. Both

[1] For instance by considering additional types of data as sensitive.

types of processing operations form part of a filing system or are intended to form part of a filing system, *ie any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis*.

The processing operations covered by data protection legislation are therefore not limited to electronic files or databases, but also include the processing of data in a manual paper file as soon as this is structured according to certain criteria.

According to Group 29, the concept of processing also includes the operations performed by Internet software and hardware without the knowledge of the data subject, and hence invisible to them, such as the use of cookies. The exchange of information related to the use of browser software is also to be considered as processing.[1]

The exact scope of the processing can, however, vary between Member States.

See exceptions and particularities under national laws (Grid 3).

1.3.6 Controller/co-controllership/processor

The **controller** is, according to the Directive, the natural or legal person who alone, or jointly with others, determines[2] the purposes and means of the processing of personal data. It is important to identify who the controller of any processing is, since this controller is the one liable for the legality of the processing and the fulfilment of the obligations towards the national data protection authority and the data subjects.

The **processor** is, according to the Directive, the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller. These will typically be a specialised third-party company that is entrusted by the controller to conduct the technical aspects of the processing, such as the sorting or the combination of the personal data.

The employee of the controller in charge of the security and management of the computer system is not to be considered as a processor.

The person who receives the personal data and starts to process the data on their own behalf will be considered as a controller.

---

1 Recommendation 1/99 adopted on February 23rd 1999, on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware.

2 Or, according to some national laws definitions, 'is entitled to determine'.

In the following paragraphs, the use of the term controller will aim at identifying who is legally responsible for complying with the aforementioned requirements. However, in practice, it will often be the researcher(s) carrying out the project in co-ordination with the controller who will use the present guidelines and take the decisions regarding the processing of personal data.

There are differences in the terminology and criteria used by the Member States to define the concepts of controller or processor.

See exceptions and particularities under national laws (Grid 4).

1.3.7 Purpose

The term 'purpose' is a key concept in data protection regulation, defining the scope of the processing and assessing whether processing is lawful or not. The purpose refers to the aim pursued by the specific use of personal data.

The Directive and the national laws refer to scientific and statistical purposes as particular categories of purpose.[1] They provide specific rules when processing is carried out for these purposes.

In the framework of the present guidelines, a scientific purpose concerns '… *aims consisting in providing researchers with information contributing to an understanding of phenomena in fields as varied as epidemiology, psychology, economics, sociology, linguistics, political science, ecology and so on'*.[2]

Statistics refer to '*any operation of collection and processing of personal data necessary for statistical surveys or for the production of statistical results*'.[3] Based on these definitions, socio-economic research as defined in the Glossary falls within the scope of scientific research.

In both cases, taking direct decisions on a particular data subject is excluded from the processing aims.

The controller will have to define the specific and precise purpose of the project, for instance 'the study of women's position in the scientific research field within the European Union'. Since this purpose falls within the category of scientific purposes, the processing will be governed by the rules specific to this category.

---

1 The scientific and statistical purposes are defined in the glossary.

2 See Recommendation R(97) 18 of the Council of Europe, *op.cit.*

3 See Recommendation R(97) 18 of the Council of Europe, *op.cit.*

2. Recommendations

2.1 Draft outline of the processing prior to starting the processing project

Prior to the launching of a research project involving the processing of personal data, the researcher will need to describe such processing and assess whether the envisaged processing is lawful using the recommendations laid down below.

Non-compliance with most of the obligations and conditions for processing data will lead to sanctions such as criminal or administrative sanctions (including, in some legislation, the cancellation of the authorisation of processing delivered by the national data protection authority) and civil liability towards the data subjects (See Section 3). Furthermore, it is essential to be aware of the obligations and conditions even before starting the processing, since it will allow a processing in compliance with all the legal requirements.

2.2 Determine who is (are) the controller(s)

We refer to the concept defined above in Section 1.3.6. The controller(s) will be the person(s) responsible for the lawfulness of the processing and for the compliance with legal requirements. As mentioned in Section 1.3.6, the controller is, according to Article 2.d of the Directive, the natural or legal person who alone, or jointly with others, determines the purposes and means of the processing of personal data.

If the controller is not based in the territory of one of the EU Member States, they might nevertheless be subject to the application of national law, as explained in Section 2.3, and be required to appoint a representative located on the territory of the Member State corresponding to such applicable law.

Different situations need to be identified:

1. **The situation of the researcher under the authority of a legal person.**

A. When a researcher is carrying out a research project in the context of the work they perform under the authority of an institute or a university the controller may be the institute or the university. This is in spite of the fact that the researcher will be the one actually conducting the research and applying the data protection requirements. For example, if a research project involves the collection of personal data, it will generally be the researcher working for the controller who will take the necessary steps to ensure the appropriate notification of the data subject as required under data protection law (see Section 2.10.3).

B. On the contrary, when the researcher is doing research on their own account, they will be the controller.

In order to determine whether the first (A) or the second (B) situation is concerned, the following elements are relevant:

- The first situation typically applies when a contract specifies that the work performed by the researcher is done in their capacity of employee or under the control of the institute or the university, or of any other third party.
- The fact that the person for which the research is carried out reserves the exclusive right to use the results is also specific of the first hypothesis.
- However, if the researcher is pursuing personal research falling outside their employment obligations, such as the drafting of a book, they will be considered as being the controller.

2. The situation where the work is performed for the benefit of a funder, such as the European Commission, a government, or a company.

The funder can only be considered to be the controller if such funder is the one deciding on the purposes and means of the processing. In most of the situations this will not be the case as the researcher, whether a university or a consultant, generally remains free to organise its work and define the purposes and means of the processing necessary to carry out the research.

3. The situation where different researchers are carrying out a research project together.

Where several legal or natural persons carry out a research project, for example as a consortium, it will be important to determine who is responsible for which processing. This can be specified in the contractual documents. The following situations can be identified:

- One set of common processing operations is carried out by all the participants to the project. In this case:
  - either there is one participant taking the lead and defining the purposes and means of the processing. This participant

will be the controller of the processing, while the others might eventually be considered as processors.

- or all, or some of them, define together the purposes and means of processing, and they will all be considered as controllers of the processing. In such cases, different national laws may apply to the processing, according the principles described in Section 2.3.

- The participants carry out different processing operations to conduct their work in the project. In this case, they will be the controllers for the processing concerning their own part of the work. Therefore, any communication of personal data between members has to be considered as a transfer to a third party (see section 2.10.8).

4. The situation where the processing is specifically regulated by law.

The controller may also be directly identified by regulations when a specific law regulates the processing.[1] It will be necessary to check this when the processing is conducted by, or for, a public or statutory body.

2.3 Determine which law(s) is (are) applicable to the processing

Based on the information presented in Sections 2.2, 2.4 and 2.6 the researcher will determine which national law(s) will be applicable to the processing. The relevant applicable law(s) will determine the conditions of the processing, including the transfer of the personal data outside of the European Economic Area (see Section 2.10.9).

Most of the Member States have adopted criteria of application similar to the rules defined in the Directive:

Principle A: The national law applies to processing carried out in the context of activities of an establishment on its territory.[2]

[1] *Eg* this is the case under the laws of Portugal Luxembourg, Finland and Sweden.

[2] Or where the national law applies by virtue of international public law. According to Group 29, '*the place at which a controller is established implies the effective and real exercise of activity through stable arrangements and has to be determined in conformity with the case law of the Court of Justice of the European Communities. According to the Court, the concept of establishment involves the actual pursuit of an activity through a fixed establishment for an indefinite period. This requirement is also fulfilled where a company is constituted for a given period*' (Working document of May 30, 2002 on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, p. 9).

This means that the application of the law does not take into consideration the origin of the data. Belgian law would apply to the processing of data collected in an African country, provided that the processing is carried out in the context of the activities of a controller established on the Belgian territory, such as a Belgian University.

Principle B: The national law also applies to processing carried out by a controller who is not established on a territory of one of the EU Member States but makes use of equipment, automated or otherwise, situated on the territory of a Member State, unless the equipment is only used for the purposes of transit through the territory of the EU.

The present guidelines were drafted assuming that the controller would be established within the EU territory. However, in the event of the involvement in a project of a controller located outside EU territory but using equipment, one or several national laws will apply to this processing. Examples of equipment are personal computers, terminals and servers, which may be used for nearly all kinds of processing operations.[1]

Group 29 considers that the installation of cookies of other applications such as javascript, banners or spywares on computers located on the EU territory with the intention to process personal data, corresponds to the use of equipment as described here above that renders the national law applicable.[2]

However, where the controller is only using equipment such as a router for purposes of transit through a national territory, European law will not apply. A typical case where equipment is used for transit only are the telecommunications networks (back bones, cables *etc.*), which form part of the Internet, and over which Internet communications are travelling from the expedition point to the destination point.[3]

The national laws generally require, when the controller is not established in a Member State, that they appoint a representative established on its territory who will be responsible for the respect of the legal requirements imposed by law. If one of the project partners is not established in a country concerned, one of the partners established in this country could be elected as their representative.

---

1 Working document of the Group 29 of May 30, 2002 on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, p. 8.

2 Working document of May 30, 2002 on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, p.9-12.

3 Working document of May 30, 2002 on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, p. 9.

Three important principles must be kept in mind:

1. Several national laws may apply concurrently due to the fact that there are several controllers involved in the processing, and that they are established in different Member States.
2. Several national laws may concurrently apply due to the fact that Member States did not adopt the same criteria for the application of the national laws.[1]
3. National laws other than Member States' laws apply to processing already regulated by Member States' national laws. Indeed, if a foreign legislation adopts the origin of the data as criteria for the territorial application, this national law will apply concurrently to the EU Member States' law that applies by virtue of the criteria of the establishment of the controller.[2]

There are some differences between the Member States legislation on this section.[3]

See exceptions and particularities under national laws (Grid 5).

2.4 Define the processing operations

The controller must set out in a document the different operations of processing (see Section 1.3.4) it is intending to carry out. On the basis of these descriptions, the controller will assess how to comply with the conditions for processing described in Section 2.10, in particular regarding the quality of the personal data.

Moreover, under some national law, certain operations are subject to a specific regime.[4]

The use of certain means in order to collect the personal data may also entail specific rules. For instance, the recourse to unsolicited communications (spamming) either by fax, email or SMS, as well as the use of cookies or of spying software to collect personal data,

---

[1] *Eg* if a controller processes personal data relating to persons established in Greek territory for the purposes of a study carried out for a Belgian University, both Belgian law and Greek law will apply to the processing.

[2] This could be the case, for example, when the data relates to data subjects located outside of the EU, and a controller located in Belgium carries out the processing.

[3] *Eg* as to the used terminology (some refer to the wider term 'means' instead of the term of 'equipment'). Moreover, some Member States have modified the scope of the transit exemption.

[4] *Eg* Austrian (article 50) and Greek law (article 8) define a specific regime for the interconnection of files while Portuguese (article 9) and Luxembourg (article 16) laws subject the combination of data to the prior authorisation of the National Data Protection Authority[4].

are respectively subject to specific conditions.[1] Group 29 has also issued specific recommendations applicable when collecting data on the Internet (see section 2.10.3).

2.5 Determine whether the personal data will be processed by a processor

In the following cases, processors will also be involved:

- where the data are intended to be processed by third parties, other than controller's employees, for the data controller, *ie* by other participants of a project or by an organisation in charge of the technical operations of processing
- where the personal data are collected to be transferred to a statistical institute or to a research centre to perform processing operations for the controller.

To ensure data protection compliance, the controller must choose a processor providing sufficient guarantees on technical security and organisational measures (See Section 2.10.6). The controller must also make sure that the processor will implement these measures respect to the national law applicable to the processing. Therefore, most of the national laws require that the controller has a written contract with the processor, or each of the processors. This contract must set out that the processor will only act on the instructions of the controller, and it establishes the tasks and liability of the processor for the processing, the security and the confidentiality of the data.

Moreover, when the processor is located outside the EU territory, in a country that does not ensure an adequate level of protection, the transfer will be subject to specific conditions, as described in Section 2.10.9.

2.6 Define who will be the data subjects

Prior to processing the data, the researcher needs to identify who will be the potential data subjects on which the processing is conducted, with regard to:

- the fact that they are natural or legal persons. This may impact on the applicability of data protection legislation (see Section 1.3.1).

[1] Articles 5§3 and 13 of the Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector contain specific regimes in this regard, restricting the right to use these means to specific conditions. The directive has to be implemented by the member states by 31 October 31 2003.

- the fact that they are dead or alive. This may impact on the applicability of data protection legislation (see Section 1.3.1).
- their location. This might affect the relevant applicable law (see Section 2.3).
- whether they are still under a statute of minority or not. This might affect the conditions of the processing (see Sections 2.10.2 and 2.10.9).

2.7 Define what will be the purpose(s) of the processing

The controller will need to define the purpose or purposes of the processing. As already mentioned, the scope of the present guidelines is limited to purposes pertaining to the categories of scientific or statistical purposes.[1]

The controller will have to inform the data subject about the purpose(s) of processing. Indeed, the data subject needs to be given sufficient information in order to assess and anticipate what the data collected will be used for. Therefore, when defining the purpose of the processing, the researcher must, at a minimum, describe the main object of the research, *eg* a study on the causes of failure at school or a study on the evolution of women's position at work.

Moreover, the controller will have to notify the national data protection authority about the purpose(s) when this is required by the applicable national law (see Section 2.10.4).

The purpose(s) need(s) to be determined, specific and legitimate (see Section 2.10.1).

2.8 Define what categories of data will be processed

It is necessary to define what data are intended to be processed, in order to verify:

- whether they constitute personal data or anonymous data (or whether the data are intended to be rendered anonymous for further processing), in order to assess whether or not the processing is subject to the application of data protection regulations (see Sections 1.3.1 and 1.3.2).
- whether they are sensitive data, which are subject to specific conditions of processing or may be prohibited from processing (see Sections 1.3.4 and 2.10.2.b).

When deciding which data will be collected and further processed, the controller must limit these data to the extent strictly necessary to achieve the purpose of processing. This means that

[1] Which are defined in the Glossary.

personal data will only be processed when it is necessary for the research project. For example, where a researcher interviews people on a subject, it is not always necessary to record personal data about the person interviewed. Furthermore, the researcher will only process the personal data that are necessary for achieving the purpose. For example, if the research aims to analyse the behaviour of people at work, it might not be necessary to record their private addresses (see also Section 2.10.1).

2.9 Determine to whom the data will be communicated

The controller will decide to whom the data will need to be communicated in the framework of the research project. For example, the controller may envisage communicating the personal data to other research partners, to a third party who will analyse the data, or to students to whom data will be submitted for the purpose of the research. Determining to whom the data will be communicated is important when assessing the content of the information to be provided to the data subject (see Section 2.10.3) and whether this communication is lawful (see Section 2.10.8). If a recipient is located in a third country (outside the EEA), additional requirements will apply (see Section 2.10.9).

Once the personal data have been rendered anonymous, they can be freely communicated to third parties.

2.10 Assess whether the planned processing complies with legal requirements

The processing of personal data is subject to the fulfilment of conditions.

2.10.1 Conditions regarding the selection and use of the data

Any personal data that the controller needs to process for the purposes of research must meet a certain level of quality and comply with the following principles.

a) The first principle is that the **data must be collected for specified, explicit and legitimate purposes**.

This principle means that, prior to processing personal data, the controller has to clearly define the purpose(s) for which the data are to be processed. To define a purpose as 'scientific research' would not be specific enough. The purpose needs to be defined more precisely such as, for example, a 'study on European residents' choice of means of transport to work'.

The controller has to communicate precisely, in concrete terms, the purposes of the research project to the national data protection authority and to the data subjects. A secret purpose would be illegal.[1]

Each purpose needs to be legitimate, meaning that interest in the research must outweigh the interest of the data subjects in excluding their data from the processing. When assessing the likely prevalence of this, the controller should have regard to the interest of the data subjects in not having their data processed, as well as to any potential damage or distress that could be caused to the data subject because of the processing of these data. Moreover, when the purpose(s) can be achieved by different methods of processing, the controller should always prefer the one which causes least damage or is less inconvenient to the data subjects.

b) The type of personal data that must be collected has to be selected diligently. All **the personal data must be adequate and relevant and cannot be excessive**.

The data must have a logical link with the declared processing purpose(s). Indeed, to collect or make use of unnecessary data, which are not selected to fit in the processing purpose(s), is forbidden.

The controller should therefore avoid the use of personal data when the scientific work can be performed without it. Furthermore, even when the purposes can only be achieved by the processing of personal data, the controller should seek to keep the use of these data to the minimum required to carry out the research.

Additionally, the data cannot be excessive, meaning that they cannot create a disproportionate risk of undermining the data subject's interests. Useful data that are not indispensable for the research have to be considered as excessive.

c) Once the data are collected, the controller must **keep them accurate and, where necessary, keep them up-to-date**.

The controller will take all reasonable means to fulfil this duty by not processing erroneous, incomplete or obsolete data. If the

[1] A duty of information toward the data subject also exists according to the ethical guidelines for the conduct of socio-economic research. Nevertheless, as explained here, the point is not only ethical but legal. Therefore, concerning those legal aspects, these are compulsory duties and not only ethical choices. Indeed, the controller has to inform **prior** to the collect, on **the content legally stated** (its identity, the purposes and additional information such as the recipient, the fact that the data subject have correct access *etc.* See Section 2.10.3). Other types of information that may have to be provided according to an ethical point of view may be provided at another moment.

controller knows that the data are not accurate, they must be erased or rectified.

d) Another principle is that **the data must be processed fairly and lawfully**.

The controller may process personal data only if such processing is in accordance with the law and compliant with good practice.

To be lawful, the processing must respect the second chapter of the Directive (quality, legitimacy, respect for the data subject's rights, duty of notification and implementation of security measures) and other national legal requirements.

To be fair, the processing must be transparent to the data subject. This involves the controller complying with his information duty and respecting the principles of good practice described in codes of conduct (and also in these guidelines).

e) The **personal data should be stored for a limited period of time**.

In principle, the purpose for which personal data are processed will determine **the period of conservation** of these data. When the purpose of processing is achieved, and the data are not required any more for that particular purpose, these personal data must be rendered anonymous or be destroyed.

As soon as the scientific or statistical research can be performed without personal data, the need to conserve such data must be considered to have ended. For example, if the personal data are used only to inform or interview the data subjects, the data shall be rendered unidentifiable as soon as this is completed.

If the use of personal data is necessary until the end of the research project, it can be stored until that time. After the end of the project and the verification of the results, the data must be rendered anonymous or destroyed.

Most national laws allow personal data to be stored for a longer term, provided that this is in order to use the data exclusively to carry out scientific research or statistics. Nevertheless, some national laws impose supplementary conditions or formalities in order to allow longer storage.

There are some differences between Member States transposition of those principles (a to e) in their national laws.

See exceptions and particularities under national laws (Grid 6).

f) A consequence of the fact that data have to be collected for defined purposes is that **personal data cannot be further processed in a way incompatible with the initial purpose**.

This implies that the controller must only process the personal data for the purposes for which these data were collected. This rule needs to be considered together with the information and notification requirements that have been imposed on the controller. Indeed, as explained under Sections 2.10.3 and 2.10.4, the controller will have to inform the data subject and the national data protection authority on the purposes of processing. Therefore, the controller will refrain from processing personal data for purposes other than those communicated to the data subjects and to the national data protection authority.

A controller wishing to process the data for purposes distinct from the original purposes will have to satisfy the conditions for the re-use of personal data (see Section 2.10.7). Softer rules for the re-use of data for statistical or scientific purposes have generally been provided (see Section 2.10.7.c).

2.10.2 Conditions regarding the legitimacy of the processing

2.10.2.a Non-sensitive data

To qualify as legitimate, the processing needs to correspond to one of the social justifications laid down by law. A processing of personal data for research purposes is therefore not always legitimate.

The controller should ensure that the processing is covered by one of the justifications, and specify in its processing plan the legal basis on which the processing rely. Among the justifications that are laid down in most national laws, the following are the most relevant to socio-economic research projects:

a) The data subject has unambiguously given consent.

Where it is feasible, the controller should always request the consent of the data subject. The controller should ensure that the consent obtained is free, explicit, specific and unambiguous, and based on the information communicated to the data subject according to the relevant applicable law.[1] The definition of what may be considered as a valid consent may vary from one national law to another. When the data subject is a minor or a person who is not able to give their consent, the controller should obtain the consent of the person legally enabled to give it on behalf of the data subject under the relevant applicable law.

[1] For the information duty, please refer to the Section 2.10.3.

In national law, where personal data also includes data relating to legal persons, the controller should obtain the consent from the person who is legally empowered to give it in the company's name.

For evidence purposes, the consent should be obtained in writing, or in a form enabling it to later be established that consent was given (*eg* the acceptance of clicking an icon on the Internet).[1]

b) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

If the research project is carried out in the public interest, the processing could be legitimate under this social justification.

If the controller is a public authority, it may be useful to check whether the organisation can benefit from such provision under the relevant applicable national law.[2]

c) The processing is necessary to comply with a legal obligation to which the controller is subject.

d) The processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for the fundamental rights and freedoms of the data subject which require protection.

To rely on this provision, the controller should:

- identify the interests being pursued when carrying out the research project
- determine whether the interests are legitimate (they must at the least not violate any legal provision)
- verify that the effect on the rights and liberties resulting from the processing of the data subject is not disproportionate, so that these rights and liberties should prevail over the interests of the controller.

---

[1] Under Italian and German law, the consent must be documented in writing. German law provides for an exemption, where the research purpose would considerably be impaired if written consent was to be obtained.

[2] For example, under Italian, German and Danish laws, the processing by and the disclosure of personal data to public authorities are regulated separately and subject to specific conditions.

e) Besides these classical hypotheses that are generally reproduced in national laws, the controller should check whether, under the relevant applicable law, the processing may be legitimated on another basis or comply with other requirements.

See exceptions and particularities under national laws (Grid 8).

2.10.2.b Sensitive data and other types of specific data

A. The processing of sensitive data is subject to very restrictive conditions. In principle, their processing is prohibited, but may be permitted under specific circumstances.

The controller should check under which circumstances the processing might be carried out. The conditions vary from one national law to another, and depend on the category of sensitive data concerned. For example, the processing of health data is allowed under different circumstances than the processing of racial or ethnic data.

The following list (a to d) details circumstances under which the processing of sensitive data may be allowed under national laws.

a) In most national laws, the processing of sensitive data is allowed provided that the data subject has given their **consent** for processing.

The remarks relating to the obtaining of consent concerning the legitimacy requirement are still valid.

For certain categories of sensitive data, some national laws do not allow the processing of the data, even when such processing is carried out with the consent of the data subject.[1]

In addition to the consent of the data subject, the relevant national law may require the authorisation or opinion of the national data protection authority.

b) The relevant national law may also consider that sensitive data may be processed when the data subject has made them public.

In such cases, the consent of the data subject, whether explicit or tacit, may also be required under certain national laws.

[1] *Eg* judiciary data under Belgian law and Luxembourg law, genetic data under Luxembourg law (except in the context of medical field or scientific research).

c) The relevant applicable national law may also authorise the processing of sensitive data for substantial public interests[1] or allow it with the permission of the national data protection authority.[2]

d) Under some national laws, the processing of sensitive data for scientific and/or statistical purposes is allowed in specific circumstances.

B. The processing of other categories of data is also subject to specific conditions.

Specific legislation, sometimes distinct from the main data protection statute, may have been adopted with respect to the processing of sensitive data[3] or other particular data such as identification numbers or data relating to credit ratings. The controller should verify whether the data it is intending to process are subject to such specific legislation.

See exceptions and particularities under national laws (Grid 9).

2.10.3 Comply with the information duty towards data subjects

Personal data can either be obtained directly from the data subject (primary collection) or obtained from a distinct alternative source of data (secondary collection).

2.10.3.a Primary collection

Primary collection covers all situations where the personal data are collected directly from the data subject, including those where the data subject ignores or is unaware of the fact that personal data are being collected, or is not properly providing these data. For example, primary collection includes the use of software to monitor a data subject's use of a website. Similarly, when the controller collects data through observation, it is considered that these data are collected directly from that person.

In the case of primary collection, the controller or their representative (if any) must provide specific information relating to the processing. This duty does not apply where the data subject has already been informed, or already knows this information.

---

1 As in Belgium.

2 *Eg* as is the case under Dutch law.

3 This is the case in Belgian Law that regulates the use of the 'numéro de registre national' in different Royal decrees. In French law, it is provided that the use of the 'Répertoire national des personnes physiques' needs to be authorised by decree.

2.10.3.a.i Timing of the provision of information

At the latest, information should be provided at the time the data are collected. When there are several controllers for a processing, the information must only be provided once.

When data collection is by questionnaire (online or offline), information should be included with it. When the data is collected by telephone, information should be provided at the beginning of the telephone call.

2.10.3.a.ii Form of provision of the information

Although the Directive does not prescribe any requirement as to the means to be used to provide the required information, certain national laws contain peculiar rules in this regard.

2.10.3.a.iii Content of the information to be provided

The content of the information to be provided is of two types: basic (to be provided in all circumstances) and additional (to be provided depending on the circumstances).

1. Basic information

The exact basic information it is necessary to provide may vary between Member States. However, under most national laws, the basic information to be provided to the data subject is:

- **The identity of the controller or controllers and, if relevant, the identity of their representative**. This information should at least include the name, denomination or trade name and address.
- **The purposes of the processing**. As explained in Section 2.10.1, the purposes have to be specified and explicit, which means that the precise description of the scientific or statistical project is to be given. The aim of this information obligation is to indicate what the data will be used for. Any information merely indicating that the data will be used for scientific or statistical purposes is not precise enough. The data subject must have an accurate idea of what the research or the statistics will be about. It is not, however, necessary to provide a detailed description of the project, *eg* regarding the methodology used, the assumptions or the phenomena that the research might aim to put in evidence.[1]

[1] A duty of information toward the data subject exists also according to the ethical guidelines for the conduct of socio-economic research. Nevertheless, as explained here, the point is not only ethical but legal. Therefore concerning those legal aspects, these are compulsory duties and not only ethical choices. Indeed, the controller have to inform

Example: In the framework of a study regarding the factors taken into account in the process of hiring workers, the researcher might want to verify if the race of the candidate plays a decisive role in the employer's decision and include this aspect in the scope of the study. The obligation to inform will oblige the researcher to indicate the topic of the study to the persons they interview but not to reveal which phenomena the study may analyse in the scope of the study.[1]

2. Additional information

The controller has to provide additional information when it is necessary to guarantee the fairness of the processing. The controller will have to assess, on basis of the circumstances and characteristics of the processing, whether or not additional information needs to be provided to the data subject.

National laws provide different criteria for assessing whether it is necessary to provide additional information.

The processing of sensitive data may also require the provision of additional information.

The following are typical types of additional information defined by the Directive:

- **the recipients or categories of recipients** of the personal data. The controller might have to provide the identity of the recipient or the categories of recipients where it is required to ensure fair processing, or to meet any other criteria defined in the relevant national law. Such information is not required where the data are to be communicated anonymously.
- **whether replies to the questions are obligatory or not**, **as well as the possible consequences that the controller attaches to a failure to reply.** In some cases, providing personal data may be mandatory when it is legally required.
- **the existence of the right of access to the data and the right to rectify the data**. This information has to be given unless the controller is granted an exemption from the right to access by the relevant national law. Section 2.10.5.a.ii outlines national issues and the possible existence of exemptions. Some national laws also place a responsibility on the controller to provide information about the existence of a **right to object.**

---

prior to the collect, on **the content legally stated**. Other type of information that may have to be provided according an ethical point of view may be provided at another moment.

[1] *Eg* the researcher could indicate that the topic concerns a 'study regarding the factors taken into account in the process of hiring workers' but they do not have to reveal they are concerned with analysing the influence of race in this area.

The controller should check in the relevant applicable law if other additional information is imposed.

Moreover, the controller must check whether there are any additional obligations in terms of information to be provided at times other than the point of data collection.

Group 29 issued specific recommendations regarding the collection of personal data on the Internet. These recommendations detail the specific information to be provided, and the manner in which to provide them to the data subject (which goes further than the basic and additional information specified above) and for implementing other rights and obligations.[1] Furthermore, Group 29 considers that the Internet user should be informed of invisible processing performed by software or hardware on the Internet, regardless of the fact that such processing concerns personal data or not, *ie* that the information processed could be related or not to an individual.[2]

2.10.3.a.iv Exemptions

In principle, there are no exemptions to this information duty. Some Member States grant, however, very restrictive exemptions from the responsibility to provide data subjects with information in relation to primary collection.

See particularities and exceptions under national laws (Grid 10)

2.10.3.b Secondary collection

When the personal data have not been obtained directly from the data subject, the controller should, before considering how to process these personal data, assess whether they comply with the requirements for re-use of such data (see Section 2.10.7).

The controller has also to inform the data subjects about any secondary collection. The main divergence from the information duty in the context of primary collection is that, for a secondary collection, most Member States provide for an exemption from the information duty, subject to the fulfilment of specific conditions, when the processing is carried out for scientific or statistical purposes.

---

[1] Recommendation 2/2001 of 17 May 2001 on certain minimum requirements for collecting personal data online in the European Union.

[2] Recommendation 1/99 adopted on 23 February 1999 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware.

2.10.3.b.i *Timing of information delivery*

The controller (or their representative) must, except where the data subject has already been provided with the information, provide the required information to the data subject:

- at the latest at the time of recording, or
- if disclosure to a third party is anticipated, no later than the time when the data are first disclosed.

Some Member States have however adopted specific measures in this regard.

See exceptions and particularities under national laws (Grid 10).

2.10.3.b.ii Content

The content of the information to be provided is similar to the information to be provided in relation to primary collection.

2.10.3.b.iii Exemption

Most of the Member States exempt from providing prior information in the case of processing for scientific or statistical purposes, where the provision of such information proves impossible or would involve a disproportionate effort. Disproportionate effort may result when it is impossible to reach or contact data subjects[1] or when contacting all the data subjects can only be done at great expense, which is disproportionate in comparison with the risk of infringing the rights of the data subject.

Some Member States subject this exemption to the fulfilment **of specific conditions.**

See exceptions and particularities under national laws (Grid 10)

2.10.4 Comply with duties towards the national data protection authorities

2.10.4.a Notification

To ensure some kind of publicity and transparency around the existence and scope of any processing, the controller is required to provide the relevant national data protection authority with certain information regarding the processing it is planning to conduct (*ie* a notification duty) prior to carrying out the processing. The information recorded will then normally be accessible to the data subjects or third parties.

[1] *Eg* when the controller cannot easily obtain their addresses.

Usually, notification is required only once, prior to beginning the processing. However, in the United Kingdom and in Ireland, notification has to be renewed every year.

Some national laws also state that any change in any of the information provided in the notification form must be immediately communicated to the national data protection authority.

Notification simply involves providing information, and does not imply that the controller has to obtain prior authorisation for the processing. However, the national data protection authority may, based on the information provided, take measures, depending on its powers granted by the national law, if it finds the processing to be unlawful (See section 3).

The notification will generally cover the identity of the controller, the purpose of the processing, the categories of data subjects, the recipients, and the transfers to third countries. The exact content of the notification is defined by national law, and further specified by national data protection authorities.

Some national laws allow exemptions to the notification duty.

See exceptions and particularities under national laws (Grid 11)

Even when an exemption exists, the controller must make all the information normally communicated to the national data protection authority through the notification procedure, available to anyone who requests it.

2.10.4.b Prior checking

In addition to notification, some national laws require authorisation to be obtained from the national data protection authority before certain types of processing are conducted. This implies that the national data protection authority will first assess whether the processing can take place.

See cases of prior authorisation under national laws (Grid 12)

2.10.5 Respect the rights of the data subject

The data subject is generally granted certain rights with regard to the processing of their data:

- a right of access to these personal data
- a right to request the data is corrected
- a right to object to the processing of the data under specific circumstances
- in some cases, a right to revoke consent given to the controller for the processing of these data.

The controller should therefore anticipate the likely exercising of these rights, and take the necessary technical and organisational measures to ensure the effective exercising of these rights by the data subjects.

2.10.5.a Right of access

2.10.5.a.i Content

All data subjects have the right to request specific information about their own personal data that are processed by the controller.

Upon request, (most national laws require this in writing and under some national laws possibly upon payment of a modest fee) the controller will have to provide the data subjects with the following information:

- whether or not data relating to them are being processed by the controller
- the purpose of the processing
- the categories of data and the data processed
- the recipients or categories of recipients to whom the data are disclosed
- the source of the data.

Particularities may exist in the national laws regarding the information to be provided. Some national laws extend the right of access.

2.10.5.a.ii Exemptions in the framework of scientific research and statistics

The Directive allows Member States to exempt the controller from respecting the data subject's right of access where processing is for the purpose of scientific research, or when data are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

The Directive, however, subjects the granting of such exemption to the conditions that there is clearly no risk of breaching privacy of the data subject, and the data are not used in order to take measures or decisions regarding any particular individual.

See exceptions and particularities under national laws (Grid 13)

2.10.5.b Right of rectification

2.10.5.b.i Content

Under the Directive, a data subject has the right to ask for data to be corrected, erased or blocked where their processing does not comply with the provisions of the Directive. This is particularly the case where personal data are incomplete or inaccurate.

This right means that the controller must correct, erase or block the data as required by the data subject, in a reasonable period. Some of national laws specify a period in terms of days or weeks.

Some national laws contain specific rules regarding the exercise of this right.

Blocked data cannot further be processed, used, or communicated without the consent of the data subject.

In addition, if the controller has disclosed the data to third parties, the controller has to notify them about any corrections, erasure or blocking carried out. Some national laws contain specific requirements regarding this notification duty.

The notification to a third party does not have to be performed if it proves to be impossible or involves a disproportionate effort.

Other national laws do not grant this exemption or subject the exemption to other conditions.

See exceptions and particularities under national laws (Grid 14).

2.10.5.b.ii Exemption to the right of correction

The Directive allows Member States to exempt the controller from the obligation to respect the data subject's right of correction in case of processing for purposes of scientific research, or when data are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

Few national laws provide an exemption to the right of correction.

2.10.5.c Right to object

The data subject has the right to object to the processing of their data and, where there is a legitimate objection, the controller may no longer process those data or communicate the data to recipients.

Some national laws grant an unconditional right to object to the processing under certain circumstances.

See exceptions and particularities under national laws (Grid 15).

2.10.5.d Right of revocation of the consent

Some countries provide that the consent to a processing may be revoked.

See exceptions and particularities under national laws (Grid 16).

2.10.6 Take technical and organisational measures ensuring the security and confidentiality of the personal data

The controller has the obligation to ensure the security of the personal data processed, meaning that it must be ensured that the data are not lost, altered, or accidentally destroyed.

The controller must also ensure the confidentiality of personal data, meaning that unauthorised access to, or disclosure of, the personal data, must be prevented.

Member States' national laws generally provide that the controller must implement appropriate technical and organisational measures to protect personal data against, *eg* accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. An example of an organisational measure would be the appointment of a data protection officer in charge of data protection issues. Technical measures include restricted access to the database to authorised persons, and the use of software protecting the system against viruses or hacking.

National laws also provide specific criteria governing the appropriate level of protection to be ensured, and generally refer in this regard to the requirement of the state of the art, the cost of implementation, the risks represented by the processing, and the nature of the data to be protected (for example, sensitive data require higher protection). For example, the relevancy of the appointment of a data protection officer will depend on the size and means of the controller, as well as of the level of sensitivity of the processed data.

Some national laws are even more specific and stricter in their requirements, or impose on the controller the responsibility to put in place specific measures for each organisational unit processing the data.[1]

If the controller entrusts part of the whole processing to a processor, they should ensure that the processor provides sufficient guarantees on technical security measures and

[1] Such as in Austria. Spain has a specific binding regulation on mandatory security measures for files containing personal data.

organisational measures governing the processing to be carried out, and compliance with those measures.

2.10.7 Comply with requirements regarding re-use of personal data for other purposes than the initial purposes of collection

When a controller intends to conduct processing by using data for a purpose that is distinct from the purpose(s) for which they were initially collected, they must first check whether or not this new purpose is compatible with the initial one(s).

Indeed, the conditions under which the re-use of personal data can be carried out depend on whether or not the purposes of re-use are compatible with the initial purposes for which the data were collected.

In principle, the re-use of personal data for incompatible purposes is not allowed.[1]

2.10.7.a Check regarding the compatibility of purposes

The Directive does not define what is considered as compatible.

Generally speaking, the purpose of the new processing has to be compared with the initial one(s) in order to assess whether there is a close relationship between them. A new purpose which is clearly different from the initial one(s), is considered to be incompatible. The comparison should be made at a detailed, rather than a general level. For example, the fact that both purposes of processing activities is 'scientific' is an insufficient argument for compatibility. However, where the initial purpose was for a study of European residents' choice of transport to work, a second purpose still dealing with means of transport could be held as compatible.

When assessing whether the further processing is compatible with the initial purpose(s), the controller shall also have regard to the context, the general philosophy of the secondary processing, as well as any other relevant criteria. Another situation which may render further processing incompatible is where the additional processing is to be conducted by a third party, especially if the activities of the third party are very different from those of the initial controller. For example, if the initial controller is a university and the personal data are transferred to a research centre of the Church of Scientology, the transfer to and further processing by this second organisation can be held as incompatible.

---

[1] But some countries give the possibility to the controller to re-use the personal data for statistical or scientific purposes, even when those purposes are incompatible with the initial ones (see section 2.10.7.c).

Some countries include other criteria in the evaluation of whether the further purpose is compatible.

2.10.7.b Conditions for the re-use of personal data for compatible processing

2.10.7.b.i Re-use of the data that the controller collected themselves

If the controller intends to use the data for another purpose which is compatible with the initial one(s), the data may be kept and further processed for the purposes of this second project.

Obviously, the data must still be available: either both the first project has not ended and the personal data have not been yet erased, or the conditions mentioned earlier for longer storage are met (see Section 2.10.1 (e)).

The controller is generally not required to re-inform the data subject or notify the national data protection authority. However, some national laws may impose on the controller to notify any modification in the processing (see Section 2.10.4).

Nevertheless, the controller will have to conduct a new analysis of the adequacy and relevancy of the personal data processed with regard to the purpose of the new processing. If some personal data are not necessary to achieve the second purpose, they need to be destroyed or rendered anonymous. The data must not be excessive, as explained above (see Section 2.10.1 (f)), and the new processing must still be lawful and fair.

2.10.7.b.ii Re-use of data obtained from a third party

When the controller obtains data from a third party, steps should be taken to verify the compatibility of the purposes of processing. This check can be done on the basis of the information originally provided to the data subject by the third party, or the content of the notification made by this third party to the national data protection authority. Where the initial controller was exempted form the notification and / or from the information duty, this check cannot be performed by reference to their content.

If the processing is compatible with the initial purpose(s), the new controller will have the right to receive and process the personal data under the same conditions as those described above relating to the re-use of the data that the controller collected himself. However, since the controller is distinct from the one who collected the data, they need to inform the data subject of the processing according to the principles applicable in the case of secondary collection (see Section 2.10.3). Moreover, the controller will have to notify the national data protection authority.

It cannot be excluded that where the personal data are provided by a third party such provider imposes specific restrictions on the processing of the data. For example, it may be that a national institute of statistics only provides personal data or coded data upon specific conditions or restriction as to the use that can be made of such data.[1]

2.10.7.c Re-use for further incompatible processing

Normally, it is forbidden to re-use data for a further project if the new purpose(s) is / are incompatible with the initial one(s).

However, the Directive grants the possibility to the Member States to consider the further processing of personal data for historical, statistical or scientific purposes as generally not incompatible with the purposes for which the data have previously been collected.

The Directive subjects this possibility to the adoption of adequate safeguards, such as the prohibition to use the personal data in support of measures or decisions regarding particular individuals.

Most of the Member States provide for this exemption when the further processing relates to scientific or statistical purposes. Therefore, it may be possible for the controller to re-use the data even when the new purpose of the further processing is scientific or statistical despite the fact that it is different from the initial purpose(s). In order to comply with the conditions for enjoying the exemption, and to know the formalities which are obligatory, the controller must refer to the relevant national law.

This exemption will only offer the right to unblock the data and avoid a new collection. Since the new project is considered as a new processing, all the legal duties relating to a new processing will have to be fulfilled in regards to the quality of the data and the legitimacy of the processing.

Therefore, the controller will still have the duty to inform the data subject unless the national law provides for an exemption. In this regard, the situation of the controller who re-uses data that they collected themselves may be different from the one of the controller who receives data from a third party. Indeed, where the latter can enjoy specific additional exemptions proper to secondary collection, the former will always have to inform the data subject unless the information regarding the processing has already been provided to the data subject (see Section 2.10.3).

---

[1] See, for example, the Commission Regulation (EC) No 831 / 2002 of 17 May 2002 implementing Council Regulation (EC) No 322 / 97 on Community Statistics, concerning access to confidential data for scientific purpose, Official Journal L 133 , 18 / 05 / 2002, P. 0007–0009.

The controller will also have to notify the national data protection authority about this new processing.

See exceptions and particularities under national laws (Grid 7).

2.10.8 Comply with the conditions for communication of personal data to third parties or recipients

The controller should refrain from publishing personal data or otherwise making them public. In most cases this will not be necessary to achieve the purpose of the research, or it may create an attempt to the data subject's interests that appears to be disproportionate to the interest of the controller.

The transfer or disclosure of personal data to third parties or recipients is a processing operation and, as such, is subject to the legal requirements of processing. Therefore, as explained under Section 2.10.7, the controller should check whether or not this transfer or disclosure falls within the scope of the initial purpose or is still compatible with this purpose, in order to determine whether or not they can transfer or disclose the data. Anonymous data can be transferred without being subject to specific requirements.

For example, if the purpose of the research is to analyse the behaviour of employees in stressful situations, the data collected in this regard cannot be transferred to a pharmaceutical company for use in promoting anti-stress products.

In addition, the controller should also check whether any of the conditions allowing an exemption to their duties, as discussed in Sections 2.10.4 and 2.10.5, is not subject to the fact that the processed personal data cannot be published.

Moreover, where such transfer is allowed, the controller should ensure that the recipient body will process the data for the purposes for which the transfer took place.

Notwithstanding the above principles, some national laws contain specific provisions with regard to the transfer of personal data (or specific categories of data), in particular for scientific research or statistics.

See exceptions and particularities under national laws (Grid 17)

2.10.9 Comply with the conditions for the transfer of personal data to countries outside the EEA

The transfer of personal data outside the European Economic Area is governed by specific conditions that need to be met in

addition to the requirements for the transfer of personal data to the recipient (see Section 2.10.8).[1]

The controller should refrain from transferring personal data to a recipient, *eg* a university, located in non-EEA countries if the country involved does not ensure an adequate level of protection.[2] At the date of drafting these guidelines Hungary, Argentine, Guernsey and Switzerland have been acknowledged by the European Commission as ensuring an adequate level of protection. Regarding the other countries, it is up to the controller to assess whether or not they are offering an adequate level of protection.[3]

Even where the transfer is allowed, additional requirements may be imposed on the controller by the national law.[4]

The Directive provides some exemptions to the prohibition of transfer of personal data to countries not offering an adequate level of protection. The most relevant exemptions contained in most of the national laws with respect to processing for research and statistical purposes are the following:

---

1 The European Court of Justice rules that there is no transfer of data to a third country '*where an individual in a Member State loads personal data onto an* Internet *page which is stored on an* Internet *site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the* Internet, *including people in a third country*'. Bodil Lindqvist Case of ECJ (Case C-101/01) available on the website http://curia.eu.int

2 The adequacy of the level of protection afforded by a third country needs generally to be assessed in the light of all the circumstances surrounding a data transfer operation, in particular the nature of the data, the purpose and duration of the processing operation, the country of origin and country of final destination, the rules of law in force in the third country in question, and the professional rules and security measures which are complied with in that country.

3 The transfer to **US companies** which adhered to the US Department of Commerce's Safe Harbour Privacy Principles is also allowed. The European Commission also allows the transfer of personal data to recognise that the recipients in Canada are subject to the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act). However, the PIPED Act mainly addresses organisations that are regulated at a federal level (federal works, undertakings or businesses) and not non-profit organisations.

4 *Eg* under the laws of Luxembourg, Portugal and Italy, the controller must notify the National Data Protection Authority of the transfer, and in some cases must obtain the prior authorisation of this authority.

a) The data subject has unambiguously given their consent to the proposed transfer.

When the controller intends to share personal data with a recipient located outside of the 'safe harbours' identified above, the consent of the data subject should always be sought for this transfer. The controller should ensure that the consent obtained is free, explicit, specific and unambiguous, and is based on information communicated to the data subject according to the relevant applicable law. When the data subject is a minor or a person that is not able to give consent, the controller should obtain the consent of the person legally entitled to give this under the relevant applicable law. The consent may need to be obtained in writing under the relevant applicable national law(s) and where it is not expressly required, it is always preferable to seek written consent for the purpose of evidence.

b) The transfer is made **from a register** which, according to laws or regulations, is intended to provide information to the public and which is open to consultation either by the public in general, or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

c) The transfer is necessary or legally required on important public interest grounds

d) National laws may contain other **exemptions** to the prohibition, subject to certain conditions, particularly when the transfer is carried out exclusively for scientific or statistical purposes.

National laws may contain other exemptions to the prohibition, subject to certain conditions, particularly when the transfer is carried out exclusively for scientific or statistical purposes.[1]

(e) Moreover, Member States may authorise a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection. Here, the controller adduces adequate safeguards with respect to the protection of the privacy, fundamental rights and freedoms of individuals, and the exercise of the corresponding rights. Such safeguards may result, in particular, from appropriate contractual clauses.

The European Commission decided that an adequate level of protection could, in particular, be achieved through a **contract** between the sender and the recipient of the personal data. At the date of the drafting of these guidelines, two sets of standard

[1] As under Italian law, where the transfer is authorised if the controller complies with a code of conduct and personal practice undersigned in accordance with the law.

contractual clauses that ensure an adequate level of protection have been adopted by the European Commission (one concerns the transfer of personal data to a controller, the second the transfer to a processor). [1]

[1] These contracts can be found on the website of the Commission: http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/index.htm. Moreover, the Group 29 also issued a series of principles on the use of contractual provisions in the context of transfers of personal data to third countries (see the Working document of 22 April 1998, primarily containing the views on the use of contractual provisions in the context of transfers of personal data to third countries).

3. Sanctions

The failure to comply with the legal requirements set for the processing of personal data may be sanctioned in different ways under national laws.

The first one concerns the possibility offered to the data subject to claim damages in case of prejudice suffered from an unlawful processing of their personal data. All national laws provide for this kind of remedy for any breach of the rights guaranteed by the national laws.

The Directive allows, however, the controller not to be held liable where he proves that he is not responsible for the event giving rise to the damage.

Secondly, almost all the national laws consider that most violations of their provisions are criminal offences.[1] Therefore, they provide for criminal sanctions varying from the payment of fines to imprisonment.

Finally, most of the Member States also grants the power to the national data protection authority to take administrative sanctions against the contravening controller. These sanctions may consist, *eg* in the imposition of administrative fines or of the retrieval of the authorisation process.

[1] The Spanish Data Protection Act does not have criminal provisions. All the infringements of the Act are considered Administrative Offences and are dealt with in Administrative Procedures. The decisions of the Spanish Data Protection Authority (Agencia de Protección de Datos) can be challenged in front of the Administrative Courts. Notwithstanding, the Criminal Code defines the unauthorised access or disclosure of personal information as a criminal offence in some specific cases and, if that is the case, the Public Prosecutor and the Criminal Courts will deal with the case.

Glossary

Browser: software programs designed to, graphically display material, among other things, that is available on the Internet. Browsers communicate between the user's computer (client) and the remote computer where information is stored (Web server).

Collection: primary and secondary collection.

Cookies: computer record of information that is sent from a web server to a user's computer for the purpose of future identification of that computer on future visits to the same web site.

Data subject: person to whom the personal data relate.

Group 29: Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up pursuant to article 29 of the Directive 95/46/CE. It has advisory status and act independently. In particular its role consists in delivering opinions on the level of protection in the Union and in third countries, and in issuing recommendations on any issue concerning the protection of individuals with regard to the processing of personal data.

Legal person: person other than an individual but having a legal capacity.

Member States: Member States of the European Union at the time these guidelines were drafted.

National data protection authority: the authority within each Member State which is responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive and listed in Schedule 1.

National laws: pieces of legislation from the Member States that have been reviewed by the authors when drafting the present guidelines and listed in Schedule 2**.**

Natural person: an individual**.**

Primary collection: collection of personal data directly from the data subject, *ie* either directly provided by the data subject or obtained through observation of the data subject.

Recipient: a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not. Authorities that may receive data during a particular inquiry shall not be regarded as recipients.

Secondary processing: processing of personal data involving the re-use of data beyond the initial processing.

Secondary collection: collection of data from sources other than the data subjects themselves.

Socio-economic research: research carried out in one of the following disciplines:

- Anthropology
- Business studies, industrial relations and management studies
- Communication sciences
- Criminology
- Cultural studies
- Demography
- Economics
- Educational sciences
- Ethics in social sciences
- Geography
- Juridical sciences
- Political sciences
- Psychological sciences
- Sociology

Using one of the following methodologies:

- carrying out interviews, whether in person or by telephone or email, with individual informants or groups
- observation, including the use of ethnographic methods
- surveys
- secondary analysis of existing data
- non-medical experimental research involving human subjects
- comparative analysis, including cross-cultural research
- analytical literature surveys, scoping exercises and content analysis
- case studies
- action research
- evaluations

Scientific purpose: the aim of a scientific purpose is to provide researchers with information contributing to an understanding of phenomena in varied fields such as, but not limited to, epidemiology, psychology, economics, sociology, linguistics, political sciences.[1] The criterion implies that processing for a scientific purpose must aim at an increase of knowledge on phenomena and according to us, the purpose cannot lead to a individual decision.

Statistical purpose: any operation of collection and processing of personal data necessary for statistical surveys or for the production of statistical results.[2]

These statistical results may further be used for different purposes, including a scientific purpose. The statistical purpose cannot lead to the possibility of taking individual decisions.

Third party: a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.

[1] This definition provided in the Explanatory Memorandum of the Recommendation (97) 18 of the Council of Europe (under n°11).

[2] This definition provided by the Recommendation (97) 8 of the Council of Europe.

Schedule 1: List of National Laws

Austria:

Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 — DSG 2000)Austrian Federal Law Gazette part I No. 165/1999. Amendments: Federal Law Gazette I No. 136/2001
www.bka.gv.at/datenschutz/dsg2000e.htm

Belgium:

Consolidated text of the Belgian law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data
www.privacy.fgov.be/textes_normatifs/version_coordonnée.pdf **(in French)**
ww.law.kuleuven.ac.be/icri/documents/12privacylaw.html **(unofficial version in English)**

Secondary legislation adopted on 13 February 2001 and published in the Official Journal of 13 March 2001
www.privacy.fgov.be/normatieve_teksten/AR%20KB%2013%20fév%202001.pdf **(in French)**

Denmark:

The Act on Processing of Personal Data (Act No. 429) of 31 May 2000
www.datatilsynet.dk/include/show.article.asp?art_id=443&sub_url=/lovgivning/indhold.asp&nodate=1

Finland:

The Finnish Personal Data Act (523/1999) was given on 22 April 1999
www.tietosuoja.fi/uploads/hopxtvf.HTM

Act on the amendment of the Personal Data Act (986/2000)
www.tietosuoja.fi/uploads/p9qzq7zr3xxmm9j.rtf

France:

Law 78-17 of 6 January 1978
www.cnil.fr/frame.htm?www.cnil.fr/textes/text02.htm **(in French)**

A bill of law exists in order to adapt the law of 1978 to the European Directive 95/46.

Germany:

The Federal Data Protection Act (Bundesdatenschutzgesetz) was adopted 18 May 2001, published in the Bundesgesetzblatt I Nr. 23/2001, page 904 on 22 May 2001
www.bfd.bund.de/information/bdsg_eng.pdf

Greece:

Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended by Laws 2819/2000 and 2915/2001)
www.dpa.gr/Documents/Eng/2472engl_all.doc

Ireland:

Data Protection Act, 13th July 1988, as modified by the Data Protection Amendment, 10 April 2003
www.dataprivacy.ie/images/Compendium%20Act.pdf

Italy:

Protection of individuals and other subjects with regard to the processing of personal data Act no. 675 of 31.12.1996 (consolidated)
www.garanteprivacy.it/garante/frontdoor/1,1003,,00.html?LANG=2

Legislative decree no. 281 of 30.07.99 Provisions concerning the processing of personal data for historical, statistics and scientific research purposes
www.garanteprivacy.it/garante/frontdoor/1,1003,,00.html?LANG=2

Luxembourg:

La loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
www.etat.lu/memorial/memorial/a/2002/a0911308.pdf **(in French)**

Netherlands:

Personal Data Protection Act approved by the Senate on 06.07.2000 (O.J. 302/2000)
www.cbpweb.nl/english/en_pdpa.htm

Portugal:

Act on the Protection of Personal Data nº 67/98 of 26 October
www.cnpd.pt/Leis/lei_6798en.htm

Spain:

Organic Law 15/1999 of 13 December on the Protection of Personal Data
www.agpd.es/upload/ley_15_ingles_v2_pdf.pdf

Royal Decree 994/1999 of June 11, adopting the Rules on Security Measures for Computerised Files containing Personal Data (Official Journal nº 151 of 25 June 1999)
www.agpd.es/upload/reglamento_ingles_pdf.pdf

Ley 12/1989, de 9 de mayo, de la Función Estadística Pública (Act on the Regulation of the Public Statistical Function, not available in English)
www.agpd.es/index.php?idSeccion=85

Royal Decree 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (Statute of the Data Protection Agency — not available in English)
www.agpd.es/upload/A.5%29%20Real%20Decreto%20428-1993.pdf

Sweden:

Personal Data Act (1998:204)
www.datainspektionen.se/PDF-filer/ovrigt/pul-eng.pdf

Personal Data Ordinance (1998:1191)
http://justitie.regeringen.se/inenglish/_issues/dataprotection/personal_data_ordinance.pdf

The Data Inspection Board Code of Statutes (1998:2)
www.datainspektionen.se/PDF-filer/difs/1998-2-eng.pdf

The Data Inspection Board Code of Statutes – (1998:3)
www.datainspektionen.se/PDF-filer/difs/1998-3-eng.pdf

United Kingdom:

Data Protection Act 1998
www.dataprotection.gov.uk/dpr/dpdoc.nsf

Schedule 2: List of National Data Protection Authorities

Austria

Büro der Datenschutzkommission
Ballhausplatz 1
1014 Wien
Austria
Tel: +43 1 531 152 525
Fax: +43 1 531 152 690
Email: dskpost@bka.gv.at
Website: www.bka.gv.at/datenschutz/legal.htm

Belgium

Commission de la protection de la vie privée
Boulevard de Waterloo 115
B-1000 Bruxelles
Belgium
Tel: + 32 2 542 7200
Fax: + 32 2 542 7201 or 542 7212
Email: commission@privacy.fgov.be
Website: www.privacy.fgov.be

Denmark

Datatilsynet
Borgergade 28, 5.
DK-1300 Copenhagen K
Denmark
Tel: +45 3 319 3200
Fax: + 45 3 319 3218
Email: dt@datatilsynet.dk
Website: www.datatilsynet.dk

Finland

Office of the Data Protection Ombudsman
P.O. Box 315
FIN-00181 Helsinki
Tel: + 358 9 259 8771
Fax: + 358 9 259 87735
Email: tietosuoja@om.fi
Website: www.tietosuoja.fi

France

Commission Nationale de l'Informatique et des Libertés
Rue Saint Guillaume 21
F-75340 Paris Cedex 7
France
Tel: + 33 1 5373 2222
Fax: + 33 1 5373 2200
Website: www.cnil.fr

Germany

Der Bundesbeauftragte für den Datenschutz
Postfach 20 01 12
D-53131 Bonn (Bad Godesberg)
Tel: + 49 228 819 950
Fax: + 49 228 819 955 00
Email: poststelle@bfd.bund400.de
Website: www.bfd.bund.de

Greece

Hellenic Data Protection Authority
8 Omirou Street
10654 Athens
Tel: + 301 335 2600 10
Fax: + 301 335 2617
Email: kkosm@dpa.gr
Website: www.dpa.gr

Ireland

Data Protection Commissioner
Block 4, Irish Life Centre
40 Talbot Street
Dublin 1
Tel: +353 1 874 8544
Fax: +353 1 874 5405
Email: info@dataprivacy.ie
Website: www.dataprivacy.ie

Italy

Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121
I-00186 Roma
Tel: +39 06 6967 71
Fax: +39 06 6967 7715
Email: garante@garanteprivacy.it
Website:http://astra.garanteprivacy.it/garante/navig/jsp/index.jsp

Luxembourg

Commission nationale pour la protection des données
68, rue de Luxembourg
L-4221 Esch-sur-Alzette
Tel: + 352 2610 6020
Fax: + 352 2610 6029
Email: info@cnpd.lu
Website: www.cnpd.lu

Netherlands

College bescherming persoonsgegevens (CBP)
Prins Clauslaan 20
P.O. Box 93374
NL-2509 AJ's-Gravenhage
Tel: + 31 70 381 1300
Fax: + 31 70 381 1301
Email: info@cbpweb.nl
Website: www.cbpweb.nl

Portugal

Comissão Nacional de Protecção de Dados
R. de S. Bento, 148-3
P-1200-821 Lisboa
Tel: + 351 21 392 8400
Fax: + 351 21 397 6832
Email: geral@cnpd.pt
Website: www.cnpd.pt

Spain

Agencia de Protección de Datos
C/Sagasta, 22
E-28004 Madrid
Tel: + 34 913 996 200
Fax: + 34 913 455 699
Email: ciudadano@agpd.es
Website: www.agpd.es

Sweden

Datainspektionen
Fleminggatan, 14
9th Floor
Box 8114
S-104 20 Stockholm
Tel: + 46 8 657 6100
Fax: + 46 8 652 8652
Email: datainspektionen@datainspektionen.se
Website: www.datainspektionen.se/

United Kingdom

Mr Richard Thomas
Information Commissioner
The Office of the Information Commissioner
Executive Department
Water Lane
Wycliffe House
Wilmslow
SK9 5AF
Tel: + 44 1625 545 700 (switchboard)
Website: www.dataprotection.gov.uk

Exceptions and Particularities

Grid 1: Under section 1.3.1

Country	Definition: personal data	Legal reference[1]
Directive 95/46	Any information relating to an identified or identifiable natural person ('data subject'): ● might directly concern the data subjects (*ie* specific information about a person) or indirectly concern a person ● must relate to natural persons ● might concern persons that are alive or dead at the moment of the processing ● must allow the direct or indirect identification of the data subject.	Article 2 (a)
Austria	Data related to legal persons are also considered as personal data. Indirectly personal data: assessment is made *in concreto*, *ie* while taking into account the information which is, or is likely to be, in the possession of the controller, to identify the data subject.	Article 2, Part I, Section 4.3 Article 2, Part 1, Section 4
Belgium		
Denmark		
Finland	Data relating to members of the household or family of the data subject are also expressly considered to be personal data of the data subject.	Chapter I, Section 3 (1)
France	Data protection legislation applies to deceased persons in specific cases.	Report on the implementation of the Directive, p. 4[2]
Germany		
Greece		
Ireland	Data relating to deceased persons are expressly not considered as personal data. Indirectly personal data: assessment is made *in concreto*, *ie* while taking into account the information which is, or is likely to be, in the possession of the controller, to identify the data subject.	Section 1(1)
Italy	Data related to legal persons are also considered as personal data.	Article 1.2 c)
Luxembourg	Data related to legal persons are also considered as personal data. Data protection legislation applies to deceased in specific cases.	Article 2(e) Article 28

[1] By reference to the law implementing the Directive 95/46/CE in the country concerned (see Schedule 1 of the guidelines)

[2] Document of the Commission entitled 'Analysis and impact study on the implementation of Directive EC 95/46 in Member States' http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/technical-annex_en.pdf

Portugal	Data protection legislation applies systematically to deceased persons.	Report on the implementation of the Directive, p. 4
Spain		
Sweden	Data relating to deceased persons are expressly not considered as personal data.	Section 3
Netherlands	Assessment indirectly personal data are personal data is made *in concreto*, *ie* while taking into account the information which is, or is likely to be, in the possession of the controller, to identify the data subject.	Chapter I, Article 1.a
UK	Data relating to deceased persons are expressly not considered as personal data. Indirectly personal data: assessment is made *in concreto*, *ie* while taking into account the information which is, or is likely to be, in the possession of the controller, to identify the data subject.	Part I, Section 1

Grid 2: Under Section 1.3.4

Country	**Definition: sensitive data and specific categories of data**	**Legal reference**
Directive 95/46	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life. Data relating to offences, criminal convictions or security measures and data relating to administrative sanctions or judgements in civil cases.	Section III Article 8.1 Section III Article 8.5
Austria	The use of data concerning acts and omissions punishable by the courts or administrative authorities, and in particular concerning suspected criminal offences, as well as data concerning criminal convictions and preventative measures does not – without prejudice to para. 2 – fringe interests in secrecy deserving protection if: ● an explicit legal obligation or authorisation to use the data exists; or ● the use of such data is an essential requirement for a controller of the public sector to exercise a legally assigned function ● the legitimacy of the data application [Datenanwendung] otherwise follows from statutory responsibilities or other legitimate interests of the controller that override the data subjects' interests in secrecy deserving protection and the manner of use safeguards the interests of the data subject according to this Federal Act [Bundesgesetz].	Section 8.4
Belgium	The concept of judicial data is extended to all data related to litigation that have been submitted to courts and tribunals.	Article 8 §1
Denmark	There are specific categories of data are data related to criminal affairs, data on serious social problems and other purely private matters. The act restricts the processing of such data. Further processing of creditworthiness is subject to specific rules.	With respect to public authorities: Section 8 (1-3) and Part 5. With respect to private entities: Section 8 (4) and Part 6
Finland	The processing of data on social affiliation, social welfare benefits, creditworthiness and socially oriented actions targeted at a data subject, *eg* taking children into custody by social welfare authorities are subject to specific rules.	Chapter 3, Section 11 (2), (6). And Chapter 4, Section 20
France	Ethnic origin, data concerning health or sex life are not considered as sensitive data. '*Moeurs des personnes*' are referred to as being sensitive data.	Article 31

Germany	Judicial data are not considered as sensitive data.	Section 3(9)
Greece	The concept of judicial data is reduced to criminal charges and convictions. Membership in any society or association and data on social welfare are also sensitive data.	Article 2(b) Article 2(b)
Ireland	The judicial data are defined as the commission or alleged commission of any offence by the data subject and any proceedings for an offence committed or alleged to have been committed by the data subject and the disposal of such proceedings or the sentence of any court in such proceedings.	Section 1(1)
Italy	In addition to data revealing political opinions, religious or philosophical beliefs, data revealing 'other beliefs' are also held as sensitive data.	Article 22.1
Luxembourg	The processing of genetic data is subject to specific rules.	Article 6
Portugal	The processing of genetic data is also subject to specific rules.	Article 7.1
Spain		
Sweden		
Netherlands	Personal data connected with 'unlawful or objectionable conduct for which a ban has been imposed' are considered as sensitive data.	Section 2, Article 16
UK	The concept of judicial data is reduced to the committing or alleged committing of an offence and related proceedings, disposal of such proceedings and court sentences.	Part I, Section 2

Grid 3: Under Section 1.3.5

Country	**Definition: Processing / Filing system**	**Legal reference**
Directive 95/46	'Processing of personal data' ('processing') is any operation or set of operations which is performed upon personal data. This includes whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. 'Personal data filing system' ('filing system') is any structured set of personal data accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.	Article 2 (b) Article 2 (c)
Austria	The transmission of data is not included in the definition of processing and is regulated separately from the processing operations	Article 2, Part 1, Section 4.9
Belgium		
Denmark	Manual paper files are not subject to the application of the act if the controller is a public authority. Such files are subject to the application of the act: • if the controller is a private entity and • if they include data on individual private persons, on financial conditions or on other personal circumstances which can reasonably be claimed not to be made open to the public. However, in such cases the controller has no obligation to inform the data subject when collecting personal data intended to be included in manual files and the data subject has no right of access regarding these data.	Section 1 (1-2)

Finland	The term 'filing system' is defined as '*a set of personal data, connected by a common use and processed fully or partially automatically, or sorted into a card index, directory or other manually accessible form so that the data pertaining to a given person can be retrieved without unreasonable cost*'.	Section 3
France	Only certain provisions of the law are applicable to non-automated processing.	
Germany	Limits the concept of 'disclosure' to the transmission to a third party. Defines separately the concept of '*non-automated data sets*' as '*any non-automated collection of personal data which is 'similarly structured and which can be accessed and evaluated according to specific characteristics'.*	Section 3(4)3 Section 3(2)
Greece	There is no explicit requirement for the file to be structured in any way.	Article 2(e)
Ireland	The filing system is defined as any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.	Section 1(1)
Italy	The scope of applicability of the legislation is not defined or limited on the basis of the concept of a filing system.	Article 1.2 b)
Luxembourg		
Portugal		
Spain		
Sweden		
Netherlands		
UK	The term filing system is narrowly defined as a set of data that is '*structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible*'.	Part 1, Article 1

Grid 4: Under Section 1.3.6

Country	**Principle: concept of controller / processor**	**Legal reference**
Directive 95/46	'Controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law. 'Processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.	Article 2 (d) Article 2 (e)
Austria	The controller is defined as the person who determines the 'purposes' only.	Article 2, Part 1, Section 4.4
Belgium		
Denmark		

Finland	The controller is defined as the person/s, corporation, institution or foundation, or combination of them for whom the filing system is established and 'who is entitled to determine the use of the file'. There is no definition of the concept of processor, but a reference to the concept of somebody processing on behalf of the controller or on instructions set out in other definitions.	Section 3 (4) Section 32 (2)
France		
Germany	The controller is defined as any person or body collecting, processing or using personal data on his or its own behalf or commissioning others to do the same. There is no definition of the concept of processor, but a reference to the concept of somebody commissioned by the controller.	Section 3(7) Section 3(7)
Greece	The controller is defined as the person who determines the 'scope and means'.	Article 2(g)
Ireland	The controller is the person who, either alone or with others, controls the contents and use of personal data.	Section 1(1)
Italy	The controller is defined as the person who determines the 'purposes and methods of processing'.	Article 1.2 d)
Luxembourg		
Portugal		
Spain	The controller is defined as the person who determines the 'purposes, contents and use'. The processor is defined as the natural or legal person, public authority, service or any other body which alone or *jointly with others* processes personal data on behalf of the controller.	Article 3(d) Article 3(g)
Sweden		
Netherlands		
UK	The controller is defined as the person or one of the persons who determines the 'purposes and manner'.	Part I, Section 1

Grid 5: Under section 2.3

Table 2.1 provides an overview of the criteria used to determine the territorial scope of national laws, depending on the location of the controller. In the table hereunder, Principles A and B shall have the following meaning:

Principle A: The national law applies to processing carried out in the context of activities of an establishment on its territory.[1]

[1] Or where the national law applies by virtue of international public law. According to Group 29, *the place at which a controller is established implies the effective and real exercise of activity through stable arrangements and has to be determined in conformity with the case law of the Court of Justice of the European Communities. According to the Court, the concept of establishment involves the actual pursuit of an activity through a fixed establishment for an indefinite period. This requirement is also fulfilled where a company is constituted for a given period* (working document, 30 May 2002, p.9, on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites).

Principle B: The national law also applies to processing carried out by a controller who is not established on a territory of one of the EU Member States but makes use of equipment, automated or otherwise, situated on the territory of a Member State, unless the equipment are only used for the purposes of transit through the territory of the EU.

Overview of criteria used to determine territorial scope of national laws

Country	Controller established in national territory / the processing is carried out in the context of the activities of a controller established in the national territory	Controller established in another EU member's State territory[1]	Controller not established within the EU[2] / the processing is not carried out in the context of the activities of a controller established in the national territory
Austria	Principle A applies	Under Austrian law, it is the law of the location of the controller of the private sector that applies to the use of data in Austria for a purpose that cannot be ascribed to any of the controller's establishment in Austria.[3]	Austrian law applies to the use of personal data in Austria, except where the data are only *transmitted* through **Austrian territory**. The controller must appoint a representative residing in Austria.
Belgium	Principle A applies		Principle B applies but refers to the use of 'means automated or not' located on the Belgian territory. The controller must appoint a representative established in the Belgian territory.

1 In certain Member States, Principle A also applies in a state that has entered into an agreement with the European Community which contains rules corresponding to those laid down in the above-mentioned Directive and the processing is not governed by these rules (case of Denmark) or (2) Member States of the European Economic Area (EEA, *ie* the fifteen Member States of the European Union and Norway, Liechtenstein and Iceland), see the case of Germany.

2 Or for the case of UK, the controller is not established within the territory of a Member state of EEA.

3 According to Section 5 of the Austrian Act, public sector controllers are those controllers who are established legal structures, according to public law, in particular as an organ of a territorial corporate body [*Gebietskörperschaft*], or as far as they execute laws despite having been incorporated according to private law.

Controller not within the scope of para. 2 are considered controllers of the private sector according to this Federal Act [*Bundesgesetz].*

Country	Controller established in national territory / the processing is carried out in the context of the activities of a controller established in the national territory	Controller established in another EU member's State territory[1]	Controller not established within the EU[2] / the processing is not carried out in the context of the activities of a controller established in the national territory
Denmark	Danish law applies where data are processed in Denmark on behalf of a controller established in Denmark. It also applies in cases where a controller established in another Member State is also established in Denmark through a subsidiary or the like. It is not relevant whether the entity in question is defined as a legal person, but whether the entity to some extent has a permanent structure. However, in this particular case the law will only apply for the processing taking place in Denmark.	According to section 4(6) of the Danish Act, Danish law shall apply where data are processed in Denmark on behalf of a controller established in another Member State and a directive does not govern the processing. Danish law shall also apply if data are processed in Denmark on behalf of a controller established in a state which has entered into an agreement with the European Community, and which contains rules corresponding to those laid down in the above-mentioned directive and the processing is not governed by these rules.	Danish law applies to a controller who is *established in a third country* (outside the EU and which has not entered into an agreement with the European Community which contains rules corresponding to those laid down in the above-mentioned Directive), if the collection of data in Denmark takes place for the purpose of processing in a third country. In the first hypothesis (a controller who is established in a third country), the controller must appoint a representative established in the territory of Denmark. Principle B also applies.
Finland	Finnish law applies when the controller is established in Swedish territory, or is subject to Finnish law.[1]		Principle B applies but refers to the use of 'means' located on the territory. Where the Finnish law applies, it requires the appointment of a representative established in Finland.
France	French law applies to processing operations located on the French territory.[2]		
Germany	Principle A applies	German law applies when the controller is established in another state of the EU or of the EEA[3] and the data are collected, processed or used by a branch in Germany	German law applies when a controller who is not located in the EU or in the EEA collects, processes or uses personal data in Germany except in case of a *storage media* only for a purpose of transit through *Germany*.

[1] In the practice, it seems however that this Member States applies Principle A instead of the principles contained in their law (see document of the Commission entitled 'Analysis and impact study on the implementation of Directive EC 95/46 in Member States' http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/technical-annex_en.pdf, p.6).

[2] The French law does not contain any provision providing criteria of territorial scope of application. It seems, however, that the principle of localisation of the processing operations is applied (see document of the Commission entitled 'Analysis and impact study on the implementation of Directive EC 95/46 in Member States' http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/technical-annex_en.pdf, p.7).

[3] European Economic Area.

Country	Controller established in national territory / the processing is carried out in the context of the activities of a controller established in the national territory	Controller established in another EU member's State territory[1]	Controller not established within the EU[2] / the processing is not carried out in the context of the activities of a controller established in the national territory
Greece	Greek law applies to any processing of personal data carried out by a controller **or a processor** established in the Greek territory, or in a place where Greek law applies by virtue of public international law.[1]	Greek law applies to any processing of personal data carried out by a controller who is not established in the Greek territory or in a place where Greek law applies, **when such processing refers to persons established in Greek territory** (the controller must appoint a representative established on Greek territory).	Greek law applies to any processing of personal data carried out by a controller who is not established in the Greek territory or in a place where Greek law applies, **when such processing refers to persons established in Greek territory** (the controller must appoint a representative established on the Greek territory). Principle B also applies and refers, regarding the transit exemption, to a transit through the Greek territory.
Ireland	Principle A applies		Principle B applies but refers to a transit through the Irish state. Where Irish law applies, the controller must appoint a representative established on the Irish territory
Italy	Italian law applies when the processing is carried out by any person whomsoever on Italian territory.	Italian law applies when the processing is carried out by any person whomsoever on Italian territory.	Italian law applies when the processing is carried out by any person whomsoever on Italian territory. Principle B also applies. Where Italian law applies, the controller must appoint a representative established on the Italian territory.
Luxembourg	Uses the criteria of the location and activities of establishment of the controller in order to apply principle A, but uses the fact that the **controller is subject to the application of the laws of Luxembourg** as criteria.		Principle B applies when a controller who is not based on Luxembourg or on any other Member State's territory and refers, regarding the transit exception to the use of 'means'. Where the law of Luxembourg applies, the controller must appoint a representative established on the territory of Luxembourg.

[1] In the practice, it seems however that this Member States applies Principle A instead of the principles contained in their law (see document of the Commission entitled 'Analysis and impact study on the implementation of Directive EC 95/46 in Member States, http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/technical-annex_en.pdf, p.6).

Country	Controller established in national territory / the processing is carried out in the context of the activities of a controller established in the national territory	Controller established in another EU member's State territory[1]	Controller not established within the EU[2] / the processing is not carried out in the context of the activities of a controller established in the national territory
Portugal	Principle A applies		Principle B applies Where the Portuguese law applies, it requires the appointment of a representative established in Portugal.
Spain	The processing is carried out on Spanish territory as part of the activities of an establishment belonging to the person responsible for the processing.		Principle B applies but refers, regarding the transit exception to the use of 'means'.
Sweden	Swedish law applies where the controller is established in the Swedish territory.[1]		Principle B applies except that the Swedish law does not apply to a transfer to third countries. Where the Swedish law applies, it requires the appointment of a representative established in Sweden.
Netherlands	Principle A applies.		Principle B applies but refers to the use of 'means automated or not' instead of 'equipment'. Where the Dutch law applies, it requires the appointment of a representative established in the Netherlands.
UK	Principle A applies.		Principle B applies when the controller is established outside the EU and EEA. The exception of the transit rule applies to transit through the UK territory. Where UK law applies, the controller must appoint a representative established in the UK.

[1] However, in practice it seems that this Member State applies Principle A instead of the principles contained in their law (see document of the Commission entitled 'Analysis and impact study on the implementation of Directive EC 95/46 in Member States' http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/technical-annex_en.pdf, p.6)

Grid 6: Under section 2.10.1

Country	Principle: Conditions regarding the selection and use of the data	Legal reference
Directive 95/46	Member States shall provide that personal data must, under the responsibility of the controller, be: (a) processed fairly and lawfully (b) collected for specified, explicit and legitimate purposes (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.	Article 6
Austria	(e) There is no exemption allowing the storing of data after the end of the project.	Article 2, Part 2, Section 6.1, 5°
Belgium		
Denmark		
Finland	(e) If the data file is significant for purposes of scientific research, the national archives can grant a permit for the data's archiving by the private organisation that collected the data, or for the transfer to an institution of higher education or to a research institute or authority operating on a statutory basis. The permit of the national archives is granted after the national data protection authority has given its opinion.	Sections 14 (4) and 35 (2)
France	The law provides for fewer conditions than in the Directive. French law only: (a) prohibits the *collection* of the data in an unfair or unlawful way (b) requires that the purpose is mentioned in the notification to the French data protection authority (d) provides for an obligation to complete and correct the file when data are incomplete or inaccurate (e) provides for a limitation of the storage in time but allows personal data to be stored for a longer term, provided that this is in order to use the data exclusively to carry out scientific research or statistics. The controller has to select for storage only those data which are needed for the purpose of scientific research or statistics. Data without scientific or statistical interest has to be destroyed.	 Article 25 Article 37 Article 28
Germany	Some principles are added to those mentioned in the Directive, *eg* that the data should be collected from the data subject. (e) There is no exemption allowing the storing of data after the end of the project.	Article 4(2)
Greece	(e) The controller must request an authorisation from the national data protection authority to store the data for a longer term than necessary for the purpose of processing in case of a processing for historical, scientific or statistical purposes.	Article 4.1(d)

Ireland	● The principle that the data must be accurate, complete and kept up to date does not apply to back up data (data kept only for the specific and limited purpose of replacing other data in the event of their being lost, destroyed or damaged). ● While those rules apply for automatic processing, it will apply only to new manual records created as of July 2003 and to existing manual records as of October 2007). ● It is allowed to store the data for a longer term when they are kept for statistical, research or scientific purposes and the keeping of which complies with such requirements (if any). This is so they may be prescribed for the purpose of safeguarding the fundamental rights and freedom of data subjects, at the condition that the data are not used in such a way that damage or distress is, or likely to be, caused to any data subject.	Section 2(4) Section 36 (5) Section 2 (5)
Italy	(e) Personal data may be stored for a longer term, provided that this is in order to use the data exclusively to carry out scientific research or statistics.	Article 9.1-bis
Luxembourg		
Portugal	(e) The storing for historical, statistical or scientific purposes, for longer periods may be authorised by the national data protection authority in case of legitimate interest.	Article 5.2
Spain	Spanish law provides for specific guarantees regarding the use of personal data for statistical purposes contained in three regulations: ● Ley 12/1989, de 9 de mayo, de la Función Estadística Pública (Act on the Regulation of the Public Statistical Function, not available in English). It describes in which conditions and with which guarantees the Public bodies entrusted with the competence on statistical work must process all (and particularly personal) data. Of special interest to this respect are the Preamble and Articles 4 to 7, 10 to 28 and 48 to 50. ● Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Data Protection Act). Article 37.m) establishes the competences and powers of the Spanish Data Protection Authority (Agencia de Protección de Datos) to enforce the Ley 12/1989. ● Royal Decree 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (Statute of the Data Protection Agency — not available in English). In Article 6 it gives a more detailed outline of the functions coming from Article 37.m) of the Data Protection Act.	
Sweden	(e) Personal data to be stored for a longer term, provided that this is in order to use the data exclusively to carry out scientific research or statistics.	Section 9
Netherlands	(e) Personal data may be stored for a longer term, provided that this is in order to use the data exclusively to carry out scientific research or statistics.	Article 10.2
UK	(a) UK law provides further specifications as to how to assess whether data are processed fairly. (b) UK law provides that the purpose specification may be provided either to the data subject or to the UK Data Protection Authority. (e) For a research project, the personal data may be stored for an indefinite term as long as the data are not processed to support measures or decisions relating to particular individuals. Also, as long as the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.	Schedule I, Part II of the law, sections 1 & 2 Schedule I, Part II of the law, section 5

Grid 7: Under section 2.10.7

Country	Re-use of the data for historical, statistical or scientific purposes	Legal reference
Directive 95/46	Data collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.	Article 6 (b)
Austria	Under Austrian law, two regimes exist regarding the re-use of data for statistical and scientific purposes which were incompatible with the initial ones: ● If the processing's goal is not to obtain results in a form relating to specific data subjects and the data were publicly available or were initially lawfully collected or are only indirectly personal for the controller, the controller shall have the right to use these for other research projects. ● In any other hypothesis, the consent of the data subject or the data protection commission's permit has to be obtained or the processing must be carried out pursuant to specific legal provisions.	Article 2, Part 8, Section 46
Belgium	Further specifications are provided as to how to assess whether a secondary use of the data is an incompatible use. By reference to criteria of 'reasonable expectations' of the data subject the new processing is compatible where the data subject could reasonably expect that the data would, or could, also be used for that other purpose. Under Belgian law, if the purpose is not compatible by itself, it will be considered compatible when used for scientific or statistical purposes and where some conditions are fulfilled. The main principle is that the controller has to process anonymous data for the second project. Nevertheless, if the scientific purpose cannot be achieved through the processing of anonymous data, the controller may use coded data. The coding will be undertaken by the controller or by an intermediary organisation. The controller must take adequate measures to prevent access to the code key. If the coded data are sensitive, the data subject must be notified unless this is impossible because it involves disproportionate efforts. In this case, the controller will have to notify the data protection authority. There is no duty to inform the data subject if the data have been coded by an administrative intermediary organisation which, by virtue of law, is entrusted to gather and code personal data, and is subject to specific privacy rules. When the scientific purpose cannot be achieved with the processing of coded data, the controller may use non-coded data. In this case, the controller will have to notify the data subject and obtain their explicit consent, unless the data are public, or the duties are impossible to fulfil or involve disproportionate effort. In this case, the controller has a duty to notify the data protection authority.	Article 4 §2 Chapter II of the Royal Decree
Denmark	The re-use of personal data for purely scientific and statistical purposes is not considered to be incompatible and is therefore allowed, provided that the processing takes place in accordance with the rules laid down in the Danish Act. Any further disclosure of data may only take place with the authorisation of the national data protection authority. If the processing includes sensitive data, the controller must obtain an authorisation from the national data protection authority prior to the commencement of the re-use of data.	Section 5 (2) Section 10 Section 48-50
Finland	The re-use of personal data for incompatible purposes when the second use is made is allowed for scientific and statistical purposes without defining any specific conditions for such re-use.	Section 7

France	The French data protection authority has issued some specifications as to what is to be considered as compatible secondary use.	Report on the implementation of the Directive[1].
Germany	A public or private controller may re-use personal data for the conduct of necessary scientific research which is in the interest of a research institute. This is provided that the scientific interest substantially outweighs the data subject's interest in excluding the change of purpose, and the research purpose cannot be attained by other means, or can be achieved only with disproportionate effort.	Section 28 and Section 14
Greece	Further processing of data for statistical and scientific purpose may be admitted with the prior consent of the national data protection authority who will assess whether such processing would violate the rights of the data subjects or even of the third parties.	Article 4
Ireland	Further specifications are provided as to how to assess whether a secondary use of the data is an incompatible use by reference to a key test with three questions: ● Should the data subject be surprised to learn that a particular use or disclosure is taking place? ● Is the data only used in ways consistent with the purpose(s) for which they were obtained? ● Is the disclosure done in ways consistent with the purpose(s) for which they were obtained? The re-use and keeping of personal data is allowed for statistical, research or scientific purposes and as may be prescribed for the purpose of safeguarding the fundamental rights and freedom of data subjects. This is provided that the data are not used in such a way that are likely to cause damage or distress to any data subject.	The guide for data controllers Section 2(5)
Italy	The re-use of personal data for incompatible purposes is allowed when the second use is made for scientific and statistical purposes without any specific conditions for such re-use.	Article 9.1-bis
Luxembourg	Further processing of data for incompatible purposes when the second use is made for statistical and scientific purpose is subject to the prior consent of the national data protection authority.	4(2) and 14
Portugal		
Spain	The re-use of personal data for incompatible purposes is allowed when the second use is made for scientific and statistical purposes without defining any specific conditions for such re-use.	Article 4.2
Sweden	The re-use of personal data for incompatible purposes is allowed when the second use is made for scientific and statistical purposes without defining any specific conditions for such re-use.	Section 9 Paragraph 2
Netherlands	Dutch law provides for additional guidance as how to assess whether or not a particular secondary purpose is incompatible with the initial one. Other criteria are to be taken into account: ● the nature of the data, ● the consequences of the intended processing for the data subject ● the manner by which the data have been obtained ● and the extent to which appropriate guarantees have been put in place with respect to the data subject.	Article 9

[1] See document of the Commission entitled 'Analysis and impact study on the implementation of Directive EC 95/46 in Member States, http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/technical-annex_en.pdf, p. 9)

	The re-use of personal data for scientific and statistical purposes is allowed without any specific conditions for such re-use.	
UK	The re-use of personal data for incompatible purposes is allowed when the second use is made for scientific and statistical purposes if the data are not processed to support measures or decisions with respect to particular individuals. The data should also not be processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.	Section 33

Grid 8: Under section 2.10.2.a

Country	Principle: legitimacy of the processing for non-sensitive data	Legal reference
Directive 95/46	Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party (c) or in order to take steps at the request of the data subject prior to entering into a contract; or (d) processing is necessary for compliance with a legal obligation to which the controller is subject; or (e) processing is necessary in order to protect the vital interests of the data subject; or (f) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (g) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.	Article 7
Austria	In addition to the social justifications provided legitimating a processing provided by the Directive, the processing carried out for scientific and/or statistical purpose is legitimate provided that it complies with certain standards.	Article 2, Part 8, Section 46
Belgium		
Denmark		
Finland	The condition of (f) does not exist as such in the Finnish law which only contains specific applications of such balance of interests where: ● there is a relevant connection between the data subject and the operations of the controller based on the data subject being a client or member of, or in the service of, the controller or on a comparable relationship between the two (connection requirement) ● the data relate to the clients or employees of a group of companies or another comparable economic grouping, and they are processed within the said grouping ● processing is necessary for purposes of payment traffic, computing or other comparable tasks undertaken on the assignment of the controller ● the matter concerns generally available data on the status, duties or performance of a person in a public corporation or business, and the data is processed in order to safeguard the rights and interests of the controller or a third party receiving the data; or	Section 8

	• the data protection board has issued a permission for the same. In addition to the legitimacy cases provided by the Directive, the processing carried out for scientific and/or statistical purposes is legitimate provided that it complies with certain standards. The national data protection authority may grant permission to process to the controller to realise legitimate interests of the controller or of the recipient of the data.	Section 14
France		
Germany		
Greece		
Ireland	In addition to the social justifications legitimating a processing provided by the Directive, the following are also justifications: • to prevent injury to health or serious loss of or damage to the property of the data subject, where seeking consent is likely to result in those interests being damaged • for the administration of justice • for the performance of a function conferred on a person by or under an enactment, or a function of the Government or a Minister of the Government.	Section 2A and 2B
Italy	In addition to the social justifications legitimating a processing provided by the Directive, the processing carried out for scientific and/or statistical purpose is legitimate provided that it complies with certain standards.	Article 12.1 d)
Luxembourg		
Portugal		
Spain	Instead of the general criteria in f, the Spanish law contains specific cases in which the processing is authorised and that concern the processing of data available in public sources. In addition to other social justifications legitimating a processing, the processing without the data subject's consent is allowed where the data are contained in sources accessible to the public. In addition, their processing is necessary to satisfy the legitimate interest pursued by the controller or that of the third party to whom the data are communicated. Unless the fundamental rights and freedoms of the data subject are jeopardised.	Article 6.2 Article 6.2
Sweden		
Netherlands		
UK	The act prohibits the processing of non-sensitive personal data unless conditions for processing set out in Schedule 2 of the Act can be met. Those are quite similar to the ones provided in the Directive. Regarding the condition of (f), Schedule 2 provides the processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject. 1. The Commissioner takes a wide view of the legitimate interest condition and recommends that two tests be applied to establish whether this condition may be appropriate in any particular case. 2. The establishment of the legitimacy of the interests pursued by the data controller or the third party to whom the data are to be. Whether the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject whose interests override those of the data controller.	Schedule 2

	The fact that the processing of the personal data may prejudice a particular data subject does not necessarily render the whole processing operation prejudicial to all the data subjects. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied. No order has been made to date.	

Grid 9: Under section 2.10.2.b

Country	Principle: legitimacy of the processing for sensitive data	Legal reference
Directive 95/46	1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life. 2. Paragraph 1 shall not apply where: (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards; or (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or (d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or (e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims [...] 4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.	Article 8
Austria	The processing of sensitive data for scientific and statistical purposes is subject to specific conditions: ● an important public interest in the research must exist ● furthermore, it must be ensured that at the recipient the data shall only be used by persons who are subject to a statutory duty to confidentiality or whose reliability in this respect is otherwise credible. The Data Protection Commission may issue its permit subject to terms and conditions in so far as this is necessary to safeguard the data subjects' interests deserving protection, in particular, with regard to the use of sensitive data.	Article 1, Part 8, Section 46

Belgium	(a) Under Belgian law, consent must be documented in writing. The processing of sensitive data for scientific research is allowed if it is carried out in conformity with specific requirements. Moreover, sensitive data, other than health and judiciary data, can be processed for statistical purposes if this is carried out in accordance with the law of July 4 1962, on public statistics.	Article 6 §2 (a) Article 6 §2 (g) and (i)
Denmark	In addition to other social justifications, sensitive data may be processed where: ● this is conducted for the sole purpose of carrying out statistical or scientific studies of significant social importance ● where such processing is necessary to carry out these studies and the data are not subsequently processed for other purposes. The data may only be disclosed to a third party with prior authorisation from the national data protection authority. The processing of civil registration numbers by private individuals and bodies is subject to specific rules under Danish law. It is allowed where this follows from law or regulations, when the data subject has given explicit consent or when the processing is carried out for scientific or statistical purposes. However, a civil registration number can not be made public without the explicit consent of the data subject.	Sections 7, 8 and 10 Article 11
Finland	The processing of sensitive data is allowed for scientific or statistical purposes without being subject to further conditions. The processing of personal identity numbers is subject to a specific regime under Finnish law and is, *eg*, allowed with the consent of the data subject or for scientific or statistical purposes.	Section 12 (1) 6 Article 13
France		
Germany	An exemption is provided regarding the processing of sensitive data for scientific or statistical purposes. The processing by a private body or public-law enterprise participating in competition, and the collection of sensitive data by a public body, is allowed where: ● this is necessary for the purposes of scientific research ● the scientific interest in carrying out the research project substantially outweighs the data subject's interest in not having their data processed for the purpose of the research, and ● the purpose of the research cannot be achieved in any other way or only in ways which would necessitate disproportionate effort.	Section 28(6)4 and Section 13(2)8
Greece	Under Greek law, the processing is subject to the receipt of a permit from the national data protection authority which is delivered only in the hypotheses specifically defined by law, where under the obtaining of the data subject's consent. The national data protection authority may permit the processing for scientific and/or statistical purpose when the processing is carried out exclusively for research and scientific purposes provided that anonymity is maintained, and all necessary measures for the protection of the persons involved are taken.	Article 7 Article 7.2(f)
Ireland	The specific conditions for processing sensitive data are added to the general condition of legitimacy for non-sensitive data and to the condition relating to the quality of the data. Therefore all those conditions must be fulfilled. If the social justification is the obtaining consent of the data subject, this consent must be explicit, *ie* based on a clear information of the purpose of the processing and supplied with that understanding. The processing is allowed if it is necessary in order to obtain information for use, subject to and in accordance with the statistic act of 1993, only for statistical, compilations and analysis purposes.	Section 2B(1)(b)(ix)

Italy	(a) In addition to the consent of the data subject, the Italian law requires the authorisation of the national data protection authority. There are specific exemptions regarding the processing of sensitive data by public non-profit-seeking bodies, allowing the processing of sensitive data for research and statistical purposes under certain conditions.	Article 22 Legislative decree N°135
Luxembourg	(a) In addition to the consent of the data subject, the Luxembourg law requires the authorisation of the national data protection authority. (e) In addition to the fact that the data subject has made the data public, the Luxembourg law requires the authorisation of the national data protection authority. The processing for scientific and/or statistical purpose is permitted when it is carried out in conformity with specific conditions, and is subject to the authorisation of the national data protection authority.	Article 14(1)(a) Article 14(1)(a) Article 6(2)(g)
Portugal	(e) Portuguese law requires that the consent of the data subject may be inferred from the fact that the data subject has made them public.	Article 7.3(c)
Spain	(a) The consent must be documented in writing when the processing concern data revealing ideology, religion and beliefs and trade union membership. Besides, there are specific provisions allowing the processing and disclosure to third parties of personal data without the consent of the data subject in the field of credit reference and in the insurance sector. The legality of the processing in both cases is subject to the adoption of adequate guarantees and, in the case of health personal data the processing needs the explicit consent of the data subject.	Article 7 Article 29
Sweden	The processing of sensitive data (excluding information relating to legal offences) for research and statistical purposes is authorised if the processing is legitimate under the criteria applicable to ordinary data. Also provided that the interest of society in the research or statistics project within which the processing is included is clearly greater than the risk of improper violation of the personal integrity of the individual that the processing may involve. If a research ethics committee has approved the processing, the prerequisites under the first paragraph shall be deemed satisfied. In a brochure issued by the Data Protection Authority about sensitive data in the research, it is explained that the research must be carried out by an established institution like a university, a high school or a private research institute. The sensitive data can be processed for research purpose without the consent of the data subject if: ● the processing is necessary for the public interest and the public interest is greater than the risk of improper violation of the personal integrity of the data subject ● if a research ethics committee approves the processing, the conditions shall be considered as being fulfilled. Under Swedish law, information about personal identity numbers or classification numbers may, in the absence of consent, only be dealt with when it is clearly justified by the purpose of the processing, the importance of a secure identification, or some other valid reason.	Section 19 Brochure on the sensitive data in the research (September 2001) Article 22
Netherlands	The prohibition of the processing of sensitive data does not apply for the purpose of scientific research or statistics and where: ● the research serves a public interest ● the processing is necessary for the research or statistics concerned ● it appears to be impossible or would involve a disproportionate effort to ask for the data subject's express consent, and ● sufficient guarantees are provided to ensure that the processing does not have a disproportionate, adverse affect on the data subject's individual privacy	Article 23

	The identification number required by law may, under Dutch law, only be processed for the purposes stipulated in such law or in administrative regulations.	Article 24
UK	The Act prohibits the processing of sensitive personal data unless one of the conditions for processing set out in Schedule 3 of the Act is met in addition to a condition set out in Schedule 2. There are additional specific conditions provided in the Statutory instrument 2000 n°417 which provides (article 9) that sensitive personal data may be processed under these circumstances: The processing: (a) is in the substantial public interest (b) is necessary for research purposes (which expression shall have the same meaning as in section 33 of the Act) (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and (d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.	Schedule 2 and 3 Statutory instrument 2000 n°417

Grid 10: Under section 2.10.3

Country	Particularities and exemptions to the obligation to inform	Legal reference
Directive 95/46	In case of primary collection (Information in cases of collection of data from the data subject) Member States shall provide that the controller or his representative must provide a data subject from whom data relating to themselves are collected with at least the following information, (except where they already has the information): (a) the identity of the controller and of his representative, if any (b) the purposes of the processing for which the data are intended (c) any further information such as: • the recipients or categories of recipients of the data • whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply • the existence of the right of access to and the right to rectify the data concerning him. In so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject. *In case of secondary collection (Information where the data have not been obtained from the data subject).* 1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any (b) the purposes of the processing (c) any further information such as:	Article 10 Article 11

	• the categories of data concerned • the recipients or categories of recipients • the existence of the right of access to and the right to rectify the data concerning him In so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject. 2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.	
Austria	The duty of information lies only with the controller, and not the representative. Additional information has to be given on the existence of a right to object. If the data are to be processed through a joint information system the controller must provide information about this. A joint information system permits collective processing by several controllers, allowing access by all controllers to the entire system, including the personal data that have been made available to the system by other controllers. In the framework of primary or secondary collection, the controller does not have a duty to provide information if exempt from the notification duty (see Section 2.10.4), *eg* if the data are already published. In the framework of secondary collection, the controller may be exempted from the information duty if: • it proves to be impossible to carry out because the data subjects cannot be reached • considering the improbability of infringements of the data subjects' rights and the expense involved in reaching the data subjects, an unreasonable effort would be required to carry out this information duty. In particular, this applies in the context of collection of personal data for purposes of scientific research or statistics.	Section 24 Section 24 Section 24.2 Section 24.4 Section 24.3
Belgium	In the framework of primary collection, the controller should provide: • additional information on the existence of the right of access to and the right to rectify the data concerning them • information about the existence of a right to object to the processing for the purpose of direct marketing. In the framework of secondary collection, and, in particular, the context of the collection of personal data for statistical purposes or historical or scientific research, the controller may be exempted from the information duty if the provision of such information appears to be impossible or involves a disproportionate effort. The controller has to notify the Belgian Data Protection Authority, stating the reasons for the impossibility of information, or of the disproportionate efforts. When the controller processes the coded data for scientific or statistical purposes in a way that is incompatible with the initial purpose, there is no obligation to inform the data subject. The intermediary organisation undertaking the coding of personal data is exempted from the information obligation provided it: • is entrusted for collecting and coding personal data • is subject to specific privacy rules.	Article 9 §1 (c) Article 9 §2 Article 31 of Chapter IV of the Royal Decree Article 28 of Chapter IV of the Royal Decree Article 29 of Chapter IV of the Royal Decree

Denmark	Danish law provides criteria for assessing whether it is necessary to provide additional information. The law states that the controller must provide additional information where this is necessary to enable the data subjects to safeguard their interests. In the framework of both primary and secondary collection, the obligation to provide information does not apply where the data subject has already received the information required. Furthermore it is not necessary to provide information if the data subject's interest in obtaining this information is found to be overridden by vital interests including the interests of the data subject himself. In the framework of secondary collection the obligation does not apply where the provision of such information proves impossible or would involve a disproportionate effort. This would normally be the case when collecting data for scientific or statistical purposes (according to the preparatory works of the Danish Act).	Article 28 (1) and Article 29 (1) Section 28 (2), Section 29 (2) and Section 30 Section 29 (3)
Finland	The duty of information lies only with the controller, and not the representative. In the framework of secondary collection, the duty to provide information may be derogated from: ● if the provision of information is impossible or unreasonably difficult, or ● if it significantly damages or inconveniences the data subject or ● if the purpose of the processing of the data and the data are not used to take decisions relating to the data subject.	Section 24 Section 24 (3)
France	French law does not contain any specific obligation to inform in case of secondary collection but that this obligation is however consecrated by the French data protection authority.[1]	
Germany	The duty of information lies only with the controller, and not the representative. Under German law, the information on the recipients has to be given only if the data subject cannot reasonably foresee whether data will be transferred to such recipients. The provision of information to the data subject is not required when: ● storage or transfer is necessary for the purpose of scientific research and the information would require disproportionate effort, or ● a private controller storing personal data for their own purpose does not have to inform the subject if the data are taken from generally accessible sources and notification is not feasible on account of the large number of cases concerned, or when notification would considerably impair the business purposes of the controller of the filing system, unless the interest in notification outweighs this impairment. If the controller is a public body, it is not subject to the information duty if: ● this would require disproportionate effort or ● this would be prejudicial to the proper performance of its duties.	Section 4(3) Section 33(1) and Section 19a(1) Section 33(2)5 Section 33(2)7 Section 19a(2)2 Section 19a(3)
Greece	The duty of information lies only with the controller, and not the representative The information categories to be provided are mandatory in any case. Therefore, all types of information have to be provided.	Article 10 Article 10

[1] See document of the Commission entitled 'Analysis and impact study on the implementation of Directive EC 95/46 in Member States. http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/technical-annex_en.pdf, p. 20

	In the framework of primary collection, the information needs to be provided in an express and appropriate manner and where the assistance of the data subject is requested to collect the data, the information must be provided in writing.	Article 11
	In the framework of secondary collection, an immediate information is required and there is no provision for any specific delay where a disclosure is intended. It also provides that the data subject must be kept informed of any disclosure to third parties before it is effected.	Article 11
	If the data are to be disclosed to third parties, data subjects must be kept informed of this disclosure before it is completed.	Article 11
Ireland	In the framework of secondary collection, there is no duty of information if the processing is made for statistical purposes or for the purposes of historical or scientific research when the provision of information proves impossible or would involve a disproportionate effort.	Section 2D(4)(a)
Italy	Where the controller entrusts the processing to one or several data processors, Italian law requires that the data subject be provided with the identity of at least one data processor to enable them to exercise their right of access.	Article 10
	Italian law requires that, in addition to the description of the purposes, the controller must provide information on the modalities of processing.	Article 10
	An additional information on the existence of a right to object has to be given.	Article 10
	In the framework of primary collection, the information is provided either orally or in writing. Moreover, the data subjects from whom personal data are requested to be provided must be previously explicitly, precisely and unequivocally informed.	Article 10
	The information categories to be provided are mandatory in any case. Therefore, all types of information have to be provided.	Article 10
	In the framework of secondary collection, the exemption from the obligation to provide prior information for a processing is subject to a favourable prior opinion of the national data protection authority.	Article 10
Luxembourg		
Portugal	In the framework of primary and of secondary collection, a legal provision or a decision of the national data protection authority may waive the information obligation. In particular, this applies to processing for statistical purposes or for the purposes of historical or scientific research, when the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid by law.	Article 10.5
	If the data are collected in open network, in the framework of primary or secondary collection, the data subject must be informed. An exception is where they are already aware that personal data may be circulating on the network without security measures, and may be at risk of being seen and used by unauthorised third parties. The controller must be able to prove that the data subject has this knowledge.	Article 10.4
Spain	In the framework of primary collection, information should be provided prior to the collection.	Article 5
	In the framework of secondary collection, the information needs to be provided within three months of the recording of the data irrespective of the fact of whether the controller intends to disclose them or not. It must also be noted that this provision shall not apply: ● where explicitly provided for by law, ● when the processing is for historical, statistical or scientific purposes, or ● when it is not possible to inform the data subject, or	Article 5

	• where this would involve a disproportionate effort in the view of the Data Protection Agency in view of the number of data subjects, the age of the data and the possible compensatory measures.	
Sweden	The duty of information lies only with the controller, and not the representative. The Swedish law provides criteria for assessing whether it is necessary to provide additional information. The law states that the controller must provide additional information if it is necessary to enable the data subjects to exercise their rights. In the framework of secondary collection, the exemption from the obligation to provide prior information for processing is subject to the condition that it proves to be impossible or would involve a disproportionate effort. However, if the data is used to take measures concerning the registered person, the information shall be provided at the latest in conjunction with that happening. Information, in the framework of secondary collection, needs not be provided if there are provisions concerning the registration of disclosure of personal data in an act or some other enactment.	Section 23 Section 25(c) Section 24
Netherlands	The duty of information lies only with the controller, and not the representative. The Dutch law provides criteria for assessing whether it is necessary to provide additional information. The law states that additional information must be provided if this is necessary to guarantee that the processing is carried out in a proper and careful manner. In the framework of primary collection, information should be provided prior to the collection. In the framework of secondary collection, the exemption from the obligation to provide prior information for processing is subject to the condition that the controller records the origin of the data.	Article 33 Article 33.3 and 34.3 Article 33 Article 34
UK	The duty of information lies only with the controller, and not the representative. In the framework of primary collection, the data controller ensures so far as is practicable that the data subject has the information, is provided with the information, or has the information made readily available to him. In the framework of secondary collection, if the disclosure is to take place after a reasonable period, the information must be provided at the end of that period. In the case of disclosure within a reasonable period, the moment of duty will be the first disclosure unless, within that period, the controllers become (or should become) aware that the data are unlikely to be disclosed. IN the latter case the controller shall inform at the time when the controller becomes (or should become) aware of it.	Schedule 1 Part II, (2) Schedule 1, Part II, (2) Schedule I, Part II, 2.2

Grid 11: Under section 2.10.4.a

Country	Principle: Obligation to notify the Data Protection Authority	Legal reference
Directive 95/46	Obligation to notify the supervisory authority: 1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. 2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:	Article 18

	• where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or • where the controller, in compliance with the national law which governs him, appoints a personal data protection official, who is responsible in particular for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive • for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21(2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations. 3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register. This register is intended to provide information to the public and is open to consultation either by the public in general or by any person demonstrating a legitimate interest according to laws or regulations. 4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8(2)(d). 5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.	
Austria	Only the controller is liable for carrying out the notification duty.# Any change in any of the information provided in the notification form must be immediately communicated to the national data protection authority. No notification is required if the processing exclusively involves personal data that have been published, personal data from public registers or personal data which are only indirectly personal (anonymised or pseudonymised data).	Article 2, Part 4, Section 17.1 Article 2, Part 4, Section 17.1 Article 2, Part 4, Section 17.2
Belgium	Any change in any of the information provided in the notification form must be immediately communicated to the national data protection authority. There is no notification duty when the processing is made for the sole purpose of keeping a register which, under a legal provision, is intended for public information purposes and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.	Section 17 §7 Section 17 §2
Denmark	Any change in any of the information provided in the notification form must be immediately communicated to the national data protection authority. The processing of data for scientific purposes must only be notified if they involve the processing of data considered as sensitive data according to the Danish Act. If a notification must be filed, the controller is exempted from the notification fee when the processing takes place exclusively for scientific or statistical purposes.	Section 46 Section 48, 50 (1), 63 (2) and 63 (4)
Finland	Only the controller is liable for carrying out the notification duty. The law grants an exemption for processing carried out for scientific or statistical purposes, except where the processing involves sensitive data	Section 36 (1) Section 36 (4)

	or implies a transfer to a country that does not ensure an adequate level of protection.	
France		
Germany	Only the controller is liable for carrying out the notification duty. If a data protection officer has been appointed, the notification is not required anymore unless the controller stores the data in the course of business for the purpose of transfer or for the purpose of anonymised transfer. The duty of notification shall also not apply if the controller processes the data for its owns purposes, provided that a maximum of four employees are concerned with the processing and consent has been obtained from the data subject.	Section 4d(1) Section 4d(4) Section 4d(3)
Greece	Only the controller is liable for carrying out the notification duty. Any change in any of the information provided in the notification form must be immediately communicated to the national data protection authority. Notification is also needed when distinct files owned by several controllers or several files serving different purposes owned by one controller are linked.	Article 6 Article 6.4 Article 8.2
Ireland	The processor is also required to take part in these notification formalities. Any change in any of the information provided in the notification form must be immediately communicated to the national data protection authority. The notification duty depends on the kind of activity of the controller or on the kind of data processed. In terms of activity, the duty of notification exists only for public sector bodies, financial institutions and insurance companies. Other kinds of controllers do not need to notify unless they process sensitive data. The notification might be refused and, in this case, the controller cannot carry out the processing. The national data protection authority may refuse the notification if: ● the details put forward by the applicant are insufficient ● other information requested by the Commissioner has not been forthcoming ● the applicant is likely to contravene any of the provisions of the Act. If the data controller holds sensitive types of data, then the Commissioner must not accept the application unless they are satisfied that appropriate safeguards for the protection of the privacy of the individuals concerned will be provided. But, while the notification process is pending, the controller may start the processing. Remark: The notification (or registration) process is likely to be reviewed shortly.	Section 16 Sections 16 to 19
Italy	Only the controller is liable for carrying out the notification duty, but the processor is also required to take part in these notification formalities. Any change in any of the information provided in the notification form must be immediately communicated to the national data protection authority. When the processing is carried out for scientific or statistical purposes and complies with certain requirements, the notification may be simplified. There is an exemption from the notification duty when the processed data are drawn from public registers, or if the processing is part of the national statistics program or statistical measures provided by law.	Article 7.1 and 7.3 Article 7.2 Articles 7.5-bis and 5-ter

Luxembourg	There is no notification duty when the processing is made for the sole purpose of keeping a register which, under a legal provision, is intended for public information purposes and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest. The duty shall also be exempted if a data protection officer has been appointed.	Article 12(3)
Portugal	The processing for the sole purpose is to keep of a register which is intended to provide information to the public and which is open to consultation by the public in general or by any person demonstrating a legitimate interest shall be exempted from notification. Moreover, the national data protection authority may allow simplified notification procedures, or an exemption of notification, if the processing is unlikely to adversely affect the rights and freedoms of the data subjects. The manual processing does not have to be notified.	Article 27
Spain		
Sweden	Only the controller is liable for carrying out the notification duty. Any change in any of the information provided in the notification form must be immediately communicated to the national data protection authority. The duty of notification shall be exempted if a data protection officer has been appointed. The manual processing does not have to be notified. Swedish law allows the Government and the data protection authority to issue regulations concerning exemptions to the notification duty and that such regulations have been issued to quite a great extent.	Section 36 Section 6 codes of statutes Section 37 Section 36 Section 41
Netherlands	Any change in any of the information provided in the notification form must be immediately communicated to the national data protection authority. The law provides for an exemption from the notification duty in the case of processing for scientific or statistical purposes. The manual processing does not have to be notified.	Article 28 Royal Decree 250, May 7 2001. Article 27
UK	Any change in any of the information provided in the notification form must be immediately communicated to the national data protection authority. Only the controller is liable for carrying out the notification duty. There is an exemption of notification for manual processing.	Section 20 Section 18

Grid 12: Under section 2.10.4.b

Country	**Principle: Prior Checking**	**Legal reference**
Directive 95/46	1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof. 2. Following receipt of a notification from the controller the supervisory authority shall carry out such prior checks or they shall be carried out by the data protection official, who, in cases of doubt, must consult the supervisory authority.	Article 20

	3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.	
Austria	The law requires prior authorisation for the processing of sensitive data, for the purpose of providing information on the data subjects credit-worthiness and for the processing that is carried out in the form of a joint information system (as defined under Article 2, Part 2, Section 4.13).	Article 2, Part 4, Section 18.2
Belgium		
Denmark	If a public administration processes personal data for scientific or statistical purposes, the opinion of the national data protection authority must be obtained prior to processing or implementing any changes to the data. If the processing is to be carried out by a private controller, prior checking of the national data protection authority is required if the processing includes: ● sensitive data (as listed in section 7 and 8 of the Act) or ● takes place for any of the purposes mentioned in section 50 (2-5). With respect to transfers to third countries, an obligation to obtain an authorisation for such transfers only applies when the processing includes: ● sensitive data or ● takes place for any of the purposes mentioned in section 50 (1) no. 2-5. If the controller decides to make use of section 27 (4) thereby legitimising the transfer by providing sufficient safeguards an authorisation must however be obtained for all transfers regardless of the nature of the transfer or the nature of the data. However, in any event an authorisation for such transfers need not be obtained if the transfer is based upon the data subject's unambiguous consent.	Section 45 Section 50 (2) and section 27 (4)
Finland		
France	The law provides that authorisation must be granted in a regulatory act if the processing is carried out for the state or a public body, or if the processing involves the use of the national identification repertory.	Article 15 and 18
Germany	Prior authorisation is needed for the processing of sensitive data or for processing intended to appraise the data subject's personality, including their abilities, performance or conduct, unless the data subject has given consent to this processing.	Section 4d(5)
Greece	Authorisation is needed when files containing sensitive data or using of a uniform code are interconnected.	Articles 7.3 and 8.3
Ireland		
Italy		
Luxembourg	Prior authorisation is required for: ● the usage of data for purposes other than those for which they were collected ● further processing of data for incompatible purposes when the second use is made for statistical and scientific purpose ● processing of sensitive data in some hypothesis ● processing for supervision purposes ● processing for supervision purposes at the workplaces ● combination of data ● processing related to credit status and solvency of the data subjects.	Article 14(1)(e) Article 4(2) Articles 6(2)(a), (b), (e), (g); 6(4)(b); 7(1) Article 10(1) Article 11(1) Article 16 Article 14(1)(d)

Portugal	Prior authorisation is required: ● if sensitive data are to be processed on the basis of an important public interest or of the consent of data subjects ● if some of the processed data relate to credit and solvency ● if a combination of files is involved ● if the controller wants to re-use the data for a different purpose than the one declared at the moment of collection.	Article 28
Spain		
Sweden	When the processing of sensitive data for research purposes is carried out without the consent of the data subject, and has not been approved by a research ethical committee, the controller needs to notify the national data protection authority for preliminary examination. The same applies for any processing of genetic data.	Personal data ordinance Section 10.1
Netherlands	Prior authorisation is required when the controller plans to process a number identifying people for a purpose other than the one for which the number is specifically intended with the aim of linking the data together with data processed by other controllers, or process data without informing the data subjects.	Article 31
UK		

Grid 13: Under section 2.10.5.a

Country	**Particularities and exemptions to the right of access**	**Legal reference**
Directive 95/46	Member States shall guarantee every data subject the right to obtain access from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense: ● confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed ● communication to him in an intelligible form of the data undergoing processing and of any available information as to their source ● knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1).	Article 12
Austria	The controller must inform the recipient of the data by appropriate means, in so far as this does not constitute an unreasonable effort, in particular with regard to a legitimate interest in the information, and that the recipient can still be determined.	Article 2, Part 5, Section 27.8
Belgium		
Denmark	An exemption for scientific or statistical research exists and is not subject to the fulfilment of any conditions.	Article 32 (4)
Finland	An exemption for scientific or statistical research exists and is not subject to the fulfilment of any conditions.	Article 27 (3)
France		
Germany	An exemption to the right of access is provided for scientific research carried out by a non-public controller who can benefit from an exemption regarding the information duty in the case of indirect collection.	Section 34(4)

	If the processing is conducted by a public entity, the access right is not granted if: • providing the information would be prejudicial to the proper performance of the duties of the public controller, or • if data must be kept secret in accordance with the law or by virtue of their nature, in particular on account of an overriding justified interest of a third party. If the processing is conducted by a public entity, it is provided for an exemption to the right of access for personal data stored neither by automated procedures nor in non-automated filing systems. This is insofar as the data subject supplies particulars making it possible to locate the data and the effort needed to provide the information is not out of proportion to the interest in such information expressed by the data subject.	Section 19(4) Section 19(1) paragraph 2
Greece	The controller must also inform the data subject about the logic involved in the processing. The controller must also specifically inform the data subject of any developments in the processing since the last access request.	Article 12
Ireland	There is an exemption provided for the processing made for the purpose of preparing statistics or carrying out research if: • the personal data are not used or disclosed for any other purpose and • the resulting statistics or • the results of the research are not made available in a form that identifies any of the data subject. When the personal data consists if an expression of opinion about the data subject, a copy of the opinion will be given to the data subject except if the expression of the opinion was given in confidence.	Section 5(1)(h) Section 3 (4A)
Italy		
Luxembourg	There is no provision for an exemption, but for a 'limitation' of the data subject's right, which means this right can only be exercised by the national data protection authority.	Article 29(2)
Portugal	The controller must also inform the data subject about the logic involved in the processing. An exemption exists when the data are: • used solely for purposes of scientific research, or • are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics if the data are not used for taking measures or decisions regarding any particular individual, and • there is clearly no risk of breaching the fundamental rights, freedoms and guarantees of the data subject, particularly the right to privacy.	Article 11.1(c) Article 11.6
Spain		
Sweden		
Netherlands	Where the processing is carried out by institutions or services for the purposes of scientific research or statistics, and the necessary arrangements have been made to ensure that the personal data can only be used for statistical or scientific purposes, the controller may refuse the requests of access.	Article 44.1
UK	Personal data which are processed only for research purposes are exempt from the right of access if: • they are processed in compliance with the relevant conditions, and • the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.	Section 33(4)

Grid 14: Under 2.10.5.b

Country	Principle: right of rectification	Legal reference
Directive 95/46	Member States shall guarantee every data subject the right to obtain from the controller: (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.	Article 12
Austria	The obligation to correct data applies only to those data for which accuracy is significant for the purpose of the data application. Incomplete data shall only justify correction if the errors, with regard to the purpose of the data application, result in the entire information being incorrect.	Article 2, Part 5, Section 27.1
Belgium		
Denmark	The data subject must specifically request the controller to notify the recipients of its data that have been rectified. The notification duty is not automatic. However, the controller will not have this duty, even if the data subject has requested it, if such notification proves impossible or involves a disproportionate effort.	Section 37
Finland	The notification of a rectification will be made to the recipients and also to the source of the erroneous personal data. In the practice, an exemption to the rectification duty exists when the processing is made for scientific or statistical purposes.	Section 29 (3)
France		
Germany	Personal data need to be blocked if the data subject disputes the fact that they are correct and it cannot be ascertained whether they are correct or incorrect. Blocked data may be used or communicated without the consent of the data subject if it is indispensable for scientific purposes, for use as evidence, or for other reasons in the overriding interests of the controller or a third party, and when the transfer or use for this purpose would be admissible if they were not blocked Under German law, an exemption exists regarding the right to correct data when a private controller makes the processing. According to this law, incorrect data must not be corrected, blocked or erased if they are taken from generally accessible sources when they are stored for the purpose of documentation, unless the data concerned are sensitive.	Section 35(4) and (8); Section 20(4) and (7) Section 35(6)
Greece	There is no provision requiring the controller to notify the recipient of personal data that have been corrected of such rectification.	Section 13
Ireland	Under Irish law, the notification will be made only to the recipients to whom the data were disclosed during the period of 12 months immediately before the request of the data subject.	Section 6(2)(b)
Italy		
Luxembourg	Any rectification, deletion or blocking of data carried out will be immediately notified by the controller to the recipients to whom the data have been disclosed unless this should prove impossible.	Section 28(7)
Portugal	An exemption exists when the data are used solely for: ● purposes of scientific research, or ● are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics provided that the data are not used for taking measures or decisions regarding any particular individual, and	Section 11.6

	• there is clearly no risk of breaching the fundamental rights, freedoms and guarantees of the data subject, particularly the right to privacy. The law exempts the controller from the obligation to respect the data subject's right of access in case of processing for purposes of scientific research, or when data are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.	Section 11.6
Spain		
Sweden	The controller will have to notify the recipients of the rectification of data only if the data subject requests so, or if more substantial damage or inconvenience for the data subject could be avoided by notification.	Article 28
Netherlands		
UK	The rectification right cannot be exercised by the data subject, but indirectly by a court or the data protection authority.	Articles 14 and 40

Grid 15: Under 2.10.5.c

Country	Particularities of the right of objection	Legal reference
Directive 95/46	Member States shall grant the data subject the right: (a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses. Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).	Article 14
Austria		
Belgium	The law excludes the data subject's right to object when: • the processing is legitimated by legal provision, or • when processing is legitimated by the performance of a contract to which the data subject is party, or • in order to take steps at the request of the data subject prior to entering into a contract.	Article 12 §1
Denmark	An objection from the data subject should not be taken into account if the processing is prescribed by law or takes place for scientific or statistical purposes.	It is presumed in the preparatory works of the Danish Act
Finland	This right is granted unconditionally but it is limited because it can be exercised only in certain circumstances (in cases of market research, opinion polls, public registers or genealogical research).	Article 30
France		
Germany	An unconditional right is granted when a private controller conducts the processing for market opinion research.	Section 28(4)

	The law excludes the data subject's right to object when the processing is legitimated by legal provision.	Section 20 and 35
Greece	The right to object is granted unconditionally in any circumstances.	Section 13
Ireland		
Italy		
Luxembourg		
Portugal		
Spain		
Sweden	This right is granted unconditionally but it is limited because it can be exercised only in certain circumstances: • when the processing was legitimated by the data subject's consent, or • when the data are processed for purposes concerning direct marketing.	Sections 11 and 12
Netherlands		
UK	The individual has the right to prevent any processing where that processing is causing or is likely to cause unwarranted, substantial damage or distress. Upon receipt of a written request to cease processing the data controller must cease to process the data or state on what grounds the request is unjustified *within 21 days*.	Part II, Section 10

Grid 16: Under 2.10.5.d

Country	**Particularities of the right of revocation of the consent**	**Legal reference**
Directive 95/46	Nothing provided	
Austria	The data subject may revoke, at any time, the consent given to the processing of sensitive or non-sensitive data without retroactive effect.	Section 9.6° and 8.1
Belgium	The data subject has the right to withdraw consent to the processing of sensitive data at anytime.	Article 6 §2 (a)
Denmark		
Finland		
France		
Germany		
Greece	The data subject may revoke, at any time, the consent given to the processing of non-sensitive data without retroactive effect.	Article 2(k)
Ireland		
Italy		
Luxembourg		
Portugal		
Spain	Spanish law provides that the consent to a processing of ordinary data may be revoked without retroactive effects, where there are justified grounds for doing so.	Article 3.6
Sweden		
Netherlands	The data subject may revoke, at any time, the consent given to the processing of non-sensitive data without retroactive effect	Article 5.32
UK		

Grid 17: Under section 2.10.8

Country	Principle transfer to third parties or recipients	Legal reference
Directive 95/46	'Third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data. 'Recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients (...) Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies. Whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organisation or by any other association or foundation, of a political nature. *Eg* subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons.	Article 2 (f) Article 2 (g) Considerant 30
Austria		
Belgium	The publication of personal data is allowed provided that it is limited to data the data subject has manifestly rendered public or that are related to the public character (i) of the data subject or of (ii) facts in which the data subject was or is implied.	Article 23 of the Royal Decree
Denmark		
Finland	The transfer of personal data for archiving purposes is allowed under certain circumstances and subject to specific conditions.	Section 35
France		
Germany	German law contains different provisions regarding the transfer of data and with specific conditions regarding the transfer carried out for scientific purposes. It must be pointed out to the recipient body that the transferred data may be processed or used only for the purpose for which they have been transferred.	Sections 15, 16, 20(7), 28, 29, 30 and 35 Section 4c
Greece		
Ireland		
Italy	Italian law provides for a panel of alternative specific conditions for the transfer of personal data (including the consent of the data subject) and for specific conditions with regard to the transfer to another controller or the dissemination of personal data necessary in the framework of scientific or statistics purposes.	
Luxembourg		
Portugal		
Spain	Personal data subjected to processing may be communicated to third parties only for purposes directly related to the legitimate functions of the transferor and transferee with the prior consent of the data subject. The consent for the communication of personal data to a third party shall be null and void when the information given to the data subject does not enable him to know the purpose for which the data whose communication is authorised will be used, or the type of activity of the party to whom it is intended to communicate them. The consent for the communication of personal data may also be revoked.	Article 11 of the Organic Law

	The consent shall not be required in the following cases: ● when the transfer is authorised by a law. ● when the data have been collected from publicly accessible sources ● when the processing corresponds to the free and legitimate acceptance of a legal relationship whose course, performance and monitoring necessarily involve the connection between such processing and files of third parties. In that case, communication shall be legitimate to the extent of the purpose justifying it ● when the transfer is between public administrations and concerns the retrospective processing of the data for historical, statistical or scientific purposes The person to whom personal data are communicated is obliged, by the mere fact of the communication, to abide by the provisions of this law.	
Sweden		
Netherlands	The transfer of personal data for archiving purposes is allowed under certain circumstances and subject to specific conditions.	Article 44.2
UK		