

Privacy Aspects of the NEEDS project.

**Walter M. Tvetter
Center for Information Technology
University of Oslo
August 2001**

1.0 Introduction

This paper examines the Directive 95/46/EC and the laws implementing it in the Nordic countries, with a view to its significance for directory services.

Where each entity is located and conducts its business in just one country, one can use national law, and any questions will be decided by that state's national regulatory authority. In more complex cases, such as the NEEDS project, it is important to analyze the consequences of the mixing of different laws, as will happen if an operator operates in another country.

A lot of the terms in both the Directive and in the different national laws are as of now unclear. A thing to be aware of is that the final say in interpretation is not the different supreme courts in the Nordic countries, but the EU-court. One may see different interpretations of terms in different countries the first years, until things are clarified by the EU court.

The basis of the discussions in this paper will be the Directive 95/46/EC. Since this in many ways is the framework of the different national legislations, and since they do not vary that much from it, the rules are presented in the form they have in the directive, and then national deviations from this are commented.

The different national legislations are viewed in light of their laws. Regulations, preliminary legislative texts and directions have so far only superficially been examined.

2.0 The evolution of legal regulation

Different regulation intended to safeguard the privacy of individuals has been appearing the last thirty years. In 1981, The Council of Europe passed “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”.

The EU Directive is an expansion and a stronger and more detailed regulation of the principles in the Convention.

Earlier one based most rules on an idea of a national regulatory authority that gave someone permission on beforehand. The permission was given for having or making a register. This system caused the authorities to use most of their time and energy to process applications. Time showed that almost all applications concerning non-sensitive information were approved. Thus this energy was by many considered to be wasted. Therefore the new law is based on a system where one does not apply, but merely informs the authorities (unless the processing is one of several special categories, where one sometimes still has to apply). And one informs them of processing, not the existence of registers. The regulatory authorities focus on follow-ups, control and inspection.

The Directive (95/46/EC) has been criticized for its model of regulation. Some wish it would go even further in trying to act on the misuse of personal information and concern itself less with regulating ordinary (legitimate) use. Another point made is that the scope of the law is so wide that it de facto covers almost all use of sound, pictures and text that everyone in their professional position carries out. Given that because this law in its full extent is almost impossible to abide by, a softening of the law would increase both its usefulness and the public respect for it.

The Swedish government released a report that criticized certain aspects of the Directive. It proposed a new simplified model. The EU Commission will release a report in October, about the state of the Directive.

3.0 Terms and subjects of the law

The Directive, and national legislation along with it has a set of terms defined in the beginning of the law:

3.1 Personal Data

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean 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;

The definition of personal data is very wide. Almost anything can be considered personal data. The different definitions in the Nordic legislation are more or less similar, not in words, but in the fact that they try to describe that any information that can be related to someone is personal data. The someone must be a physical person. The Swedish law only covers living persons. Danish, Finnish and Norwegian laws do not specify this, although it is assumed that they only cover living persons. The Icelandic law explicitly covers both living and dead individuals.

The Finnish law also describes personal data as something that can identify a group of people.¹

3.2 Processing personal data

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

In this definition, and in the laws of all the Nordic countries, the NEEDS catalogue is most certainly included.

More interesting is what kind of handling of information that qualifies for the term processing. If the overlaying searchengines of SUNET, UNINETT, FUNET are processing personal data, they will have to be either processors or controllers according to the law.

3.3 Personal data filing system

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

This is also defined in many different ways in the different countries, but a searchable index with people will be included in all of them. This is mainly a non-electronic record index, that can be searched by f.ex. name not date.

3.4 Controller

(d) '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;

The controller is typically the organization itself, f.ex. "The University of Oslo"

3.5 Processor

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

This can f.in. be UNINET processing personal data on behalf of the University of Oslo.

In the Swedish law this is called a "Personal data assistant" (Sec. 3), in Denmark (Sec. 3.5) it's called a "Processor", in Norway it's also called a "Processor" (Sec. 2). Finland does not have any definition of this term.

3.6 Third party

(f) '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 authorized to process the data;

This is more or less identical in all the national legislations.

3.7 Recipient

(g) '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;

The term is found in the Swedish and Danish laws, but not in the Finnish or Norwegian ones.

3.8 Consent

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Further about consent, see below.

3.9 Sensitive Data

Although the term is used in all laws but the Danish one, it is only defined in the Norwegian one.

3.10 Geographical Application

The Directives Art. 4 states that national law is applicable pursuant to the Directive.

The different laws govern the processing of data in the respective country, either by a controller based there or on equipment located there. The different national supervising authorities generally cooperate, so there is little or no reason to believe that a conflict between national laws should cause problems.

4.0 Obligations of the Controller

The obligations of the controller are many. Basically one can divide them into two categories; what he has to do to be able to process personal information, and what he has to do because he processes personal information.

4.1. Requirements for processing personal data.

The first and foremost requirement is the stating of a purpose. This purpose must be specified, explicit and legitimate². In other terms one must define, with a large degree of detail, why one needs to process personal data. This purpose will be the basis of the use of the different rules. Whether or not security routines are sufficient, whether routines for operation and maintenance are sufficient, the question of whether or not the processors need to process the information is sufficient, among other questions, will be dependent on the purpose.

The next is on what grounds one shall base the infringement of someones right to privacy on. This may well be called the core of the legislation.

European Union:

Bases its Directive 95/46/EC on both new thoughts and the Council of Europe's "Convention for the protection of individuals with regard to automatic processing of personal data". The Directive should have been implemented in the entire European Economic Area (EEA) within Oct. 24 1998. As of now, Germany, France, Ireland and Luxemburg have not yet implemented the Directive.

The Directive has six different alternate criteria for processing data (Art 7) including consent

Norway:

Has six different alternate criteria for processing data (§8) in addition to consent. Has spilt EU-Art. 7 (e) into two alternates, but apart from this is mainly a copy of the Directive.

Sweden:

The rules, in §10 are more or less identical with the directive.

Denmark:

The rules, in Sec. 6 are more or less identical with the directive, although some rules, concerning the Danish Marketing Practices Act follows. These do not affect the NEEDS project.

Finland:

Section 8: General prerequisites for processing; Follows the system of the Directive, but has nine alternate criteria (prerequisites) including consent. Two of the criteria differ from the Directive; Sec 8 (1) (5) (w.r.t. Sec 8 (2)) which gives an (adequate) connection both between the data subject, the data controller and his operations as a criteria.

Sec. 8 (1) (8) narrows the Directives Art. 7 (f) to where "the matter concerns generally available data on the status, duties or performance of a person in a public corporation or business". It is unclear whether this makes the alternative more usable within its limits.

Finnish law also gives the Data Protection Board the power to issue special permissions for

processing, Sec. 8 (1) (9) also. Sec. 43 (1).

Finnish law does not have anything equal to the Directives Art. 7 (e)'s "...exercise of official authority..."

The Finnish law also has a Sec. 17. about public registers, which in itself is independent and sufficient grounds for the processing of personal data.

Iceland:

Art. 8 of the Icelandic law is more or less identical with the Directives Art. 7.

Consent is the basis and an identical criteria in all the legislations.

One of the alternate conditions equivalent to the Directives Art. 7 and 26 must be fulfilled according to each national law. The simple and safe way of doing this is with consent. This necessitates a somewhat increased workload in processing forms of consent, but will be a lot safer in the long run.

There is a question of how one should get this consent. One possible solution is to include the consent in the employment-contract. It is doubtful whether employees without some special and rather severe reasons can refuse to be listed in a catalogue containing contact-information relating to their work. Thus one can include information with the employment-contract (to make it informed) and a section of the employment-contract concerning the subject (to make it specifically expressed). The requirement that it is to be freely given is also fulfilled, one can refuse to take the job. There is no rule that says one can demand to separate out an (unwanted) part of a contract one otherwise is pleased with.

Employees that already have their contracts will just have to be informed properly. Since the collection of consent was impossible (since this duty was unknown) before the regulation came, one can also argue that with an interpretation of their employment-contracts one can find the consent given through this.

The other common criterias are:

(b) processing is necessary for 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; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) 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

(f) 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 which require protection under Article 1 (1).

4.2. Obligations when processing personal data.

4.2.1 Security issues;

The Processor shall according to Art. 17 of the directive :

“must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.”

A publicly accessible database is already public, so confidentiality is not a very interesting question here. What is left is appropriate safeguards to ensure that the information is correct (this includes the erasing of old information). Also the duty of guarding against all other forms of unlawful processing will include the taking of measures to hinder the downloading of all or a large portion of the entries.³

4.2.2 Notification;

The controller has an obligation to notify the data protection agency when processing personal data. Most of the data protection agencies have either electronic notification or simple forms one can fill out.

Finland: Has a special rule in Sec. 36 (2) (1) where notification must be given when personal data is transferred outside the EEA, if the data is transferred on the grounds stated in Sec 22 or Sec 23 alt. (6)⁴ or (7).

4.2.3 The collection of data

When one collects personal data about someone, one must inform the data subject about this. Art. 10 regulates where one collects data from the registered himself., and Art. 11 where the data has not been obtained from the data subject.

It is important to realize that the practical use of Art. 10 is not when someone fills out an application for something and then hands it in; then they know that data is being collected.

The Art. is used f.in. on the logging of info from visitors on a web page. If this happens, for other purposes than system maintenance, one has a duty to inform the registered in advance.

Art. 11 is used where one collects data from somewhere else, f.in. from a payroll database for use in directory services.

Finland has compiled both rules into Sec. 24, Sweden has the rules in Sec. 23 and 24, Denmark has rather complicated rules that state roughly the same in §§28 and 29, and Norway has §§18 and 19.

4.4.4. Information

The controller has an obligation to inform when he processes personal data.

-To the data subject:

When the data subject is informed, f.in. where he/she is the source of data, delivered knowingly, this duty is not present. If one collects data from the data subject unknowingly (f.in. cookies) or from another source, one must inform the data subject:

One should inform the data subject of what processing of personal data one is instigating, the purpose of this, the legal grounds for processing, general information about how the processing is done, and of course which information about the subject that is being processed.

-To the general public:

This is done through the notification addressed to the Data Protection Agency

-To anyone who wishes information:

Basic information about what processing of personal data he is executing.

4.3 The use of “national identification numbers”

The Directive gives each nation the choice of regulation concerning the use of “national identification numbers”(NIN)⁵. This rule is placed with the “special categories” that is sensitive information. The nordic countries each have a separate rule regulating the use of such.

In *Norway*, the use of NIN is not viewed as the processing of sensitive data. It is however only permissible when there is “a objective need for certain identification” and “the method is necessary to achieve such identification”.

Sweden has chosen to use similar requirements, but have added the alternative “some other noteworthy reason”. This seems to indicate gentler terms.

Finland has a more complicated rule regarding the use of NIN. Here consent is the main condition. Then the law states a number of causes and conditions, a sort of collection of conditions from the Directive.

Danish law says that “official authorities” may process NIN “to unambiguous identification or as file numbers”. Others may only do this with consent, where it follows from laws or regulations, for statistical or scientific purposes and a last choice, that seems to permit it when it is usual and/or necessary for a company, institution etc. to do this.⁶

If one uses NIN to extract information from f.ex. payroll databases, this can be of importance. But as long as the NIN are not transferred out of the payroll database one can argue that processing of such is not happening (it is of course happening with the payroll database, but here it is permitted).

5.0 Rights of the data subject and others

5.1 The rights of access

According to the Directives Art. 12, the data subject has a right to access. He can demand information about whether or not data about him is being processed, what it is, how this is done, etc. The information shall be freely and swiftly given, at no expense.

In Finland (Sec. 10), Norway (§18), Sweden (Sec 26.) any physical person can access information about what kind of activities someone has with personal information processing. Denmark seems to limit this to those who actually are registered (31). To this one must add that since all processing has a duty of notification, and the notification is available to the public from the data protection authorities, the public (who are not data subjects) can still get information in Denmark.

The Finnish Sec 26 (3) gives the processor the right to charge a reasonable sum of money for access, if less than one year has passed since the last time (if any) this subject demanded this.

The Swedish law has a similar rule in Sec. 26 where a controller is liable to provide the data subject with free access once per annum.

The Danish law derogates the ability to decide this to the ministry of justice. As of now, one must pay between 10 and 200 danish kroners for access⁷.

In Norway all rights of access can be used free of charge. This is explicitly stated Sec. 17.

5.2 Rights concerning Rectification

The Directive Art. 12 (b) and (c) states that the data subject has a right to demand that all personal data about him/her is rectified, blocked or erased in the event that it is incorrect or if the grounds for processing it no longer remain. If the processor has transferred personal information to a third party, any rectification or notice of incorrect information shall result in notification to this part, unless this proves to be impossible or involves a disproportionate effort. With the NEEDS project, it is of course impossible to rectify information to the end-user. Ensuring that all sites are updated constantly then becomes even more important.

5.3 The data subjects right to object

The Directives Art. 14 gives the data subject a right to object; Art. 14 a concerns the cases where the data subject has a justified objection that relates to his/her grounds and particular situation. The article is meant to be an extra safeguard for the use of the grounds specified in Art. 7 (e) and (f). Both these alternatives are a comparison of the need for the controller to do something to what disadvantage this causes for the data subject. Art 14. (a) merely states that this comparison can be done again at any time. None of the national legislations seem to include this right on a general basis, but limits it to direct marketing and related issues.

As the grounds this is ment to safeguard against allready contain a weighing of interests, what this really says, is that every data subject has the right to have his or her interests weighed

individually. This can be found in the rules about automated decisions. As described below, Sweden has some special ways of viewing this question.

There seems to be little or no reason however, not to respect the wishes of individuals with special reasons as long as these are solid. This question comes back in relation to the publishing of personal data on the Internet.

Art. 14 (b) gives the data subject the right to object to personal data relating to him/her being used for the purpose of direct marketing (both by the controller, a third party or on behalf of a third party).

The *Norwegian* law has in § 26 a rule that grants a right to object to direct marketing. A central register has been made, where individuals can register. All who wish to conduct direct marketing have to filter their lists against this register.

The *Finnish* law states in Sec, 30 that the data subject has a right to object, but this law also widens the situations in which the data subject can object, to also include (direct marketing), market research, opinion polls, genealogical research and public registers. Whether or not directory services is included in this definition (public registers) is unclear.

The *Swedish* law has a short rule in Sec. 11 that states that only a written notice from the data subject is a valid objection to direct marketing. Concerning the publication of personal data on the Internet, the data subject has another rule about objection, see under 6.

The *Danish* law lists different categories in Art. 12 of what kind of information may be processed in direct marketing purposes. In addition Art. 36 has a CPR-register where consumers can register to avoid being contacted.⁸

6.0 International exchange of data

The Directives chapter IV concerns the transfer of personal data to third countries⁹. This is forbidden in Art. 25 where the third country does not have an “adequate level of protection” where what adequate is in any given set of circumstances, is determined by an assessment of these.

A third country is a country outside of the EU or the EEA.

When making information available on the Internet, one is de facto making them available for the entire world, thus also countries that do not provide an adequate level of protection.

Art. 26. lays down conditions for allowing the transfer of personal information to third countries without an adequate level of protection. Not all of these are similar to the Art. 7 conditions, but also here consent is the preferred condition. The others are:

- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or*
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or*
- (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or*
- (e) the transfer is necessary in order to protect the vital interests of the data subject; or*
- (f) 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.*

For the transference of personal data to third countries these conditions come in addition to the ones in Art. 7. This is because the directory will be available on the Internet, and one therefore must have fulfilled a condition for transference to a third country without adequate protection. Because of this, some of the alternate conditions in Art. 7, that could seem quite convenient, become less useful when they are not found in Art. 26.

One relevant grounds found in all of the national legislations is “to perform a contract between the data subject and the controller”. Some theoretics in Norway claim that this covers the consequences of employment contracts, and thus will replace individual consent with the employers right to decide if this is necessary. The Norwegian data protection agency does not agree with this, and claims this is solved through the general provisions – in effect that if one can publicise information within the EEC, one can also put them on the Internet (third countries). This seems to be a very practical solution, if it can be used.

Norway:

The Norwegian law does not use the term “third country”, but rather “other countries”. It then states that:

“Countries which have implemented Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data meet the requirement as regards an adequate level of protection.”¹⁰

This poses the problem that four of the EU countries have not yet implemented the Directive. And because the law prohibits transference to countries without an adequate protection, without using the term “third countries” to which one always can transfer personal information, one is left with a difficult question. Germany is in the Swedish law not a “third country”, and thus it permissible to transfer personal information here, even when Germany has not implemented the Directive. According to the Norwegian law, Germany is an “other country” and does not have adequate protection.

Furthermore, if one bases the processing on another legal basis than consent in §8, one will see that this basis is not found in § 27. However in the preliminary acts¹¹, it is clearly stated that if personal information is publicly available inside Norway, and this is within the limits of the law, there is little or no reason to give this stronger protection for publishing it outside Norway or the EEC.

Another way of putting this is that if information already has been made public within the EEC, any (and thus a non-existing) level of protection will be adequate.

Finland:

The Finnish law has a rule very similar to Art 25. (Sec 22) and one similar to Art. 26 (Sec 23). The latter one has adopted the Art. 26.2 exemption as another alternate condition alongside the others:

(7) the controller, by means of contractual terms or otherwise, gives adequate guarantees of the protection of the privacy and the rights of individuals.

The Finnish law does not address the issue of when information already is made public. The Finnish Data Protection Ombudsman's decision 12.11.1999 712/44/99 states that because personal data on the Internet can be used by anybody anywhere in the world, it is required an unambiguous consent of the data subject.

Sweden:

The Swedish law has an additional rule in Sec. 34, subsection 2. concerning the Council of Europe Convention. This states that personal data can in any case be transferred to countries that have acceded the Convention, as long as the information shall be used solely in that country.

The Swedes had very strict rules concerning third countries and the Internet when the law was passed in 1998. It became quite obvious that the rules were a bit of an overkill. The Data Inspection Board among others opted for easier and less strict rules. These were set into effect on January 1. 2001.

The Swedish system of today is based on a theory that harmless information can be put on the Internet without securing adequate levels of protection. This because if the information is harmless, then any level of protection is adequate. If using Sec. 10 (f) as grounds for processing, then one can easily, without consent put f.in. personal information relating to a persons job on the company web - page. If on the other hand the registered individual objects to this, one has to stop. This because then the information is no longer harmless.

In other words; if the data subjects in their subjective opinion of whether or not he/she feels that the processing of personal information about him/her is a violation of their rights to privacy feels this is indeed a violation, then their opinion will be decisive when using Sec. 10 (f) as grounds for processing. This then meaning that if the data subject objects one cannot process personal data with based on 10 (f) as the legal grounds.

Denmark:

Has an option for grounds important to the public, and one for the fulfillment of a contract between the data subject and the controller.

Iceland:

Iceland does not have any grounds in its law regarding public interest, the interest of the controller or anything similar.

7.0 Supervision and the national dataprotection agencies

Art. 28 states that the member states shall have at least one public authority responsible for monitoring the application of the Directive within its territory. Norway, Sweden, Denmark and Iceland have all had one such, while Finland has had two.

7.1 Notification and documentation

As described, the situation in the Nordic region is one that prescribes an act of notification before processing can commence. Before this can be done, some documentation will have to be made. This is described above, in 4.2.

The documentation shall not be added to the notification, but kept for internal use. This includes an assessment of security and risk relating to the project, routines for frequent assessment and control of this, and routines for dealing with deviations.

After this is in place, one can send the notification to the dataprotection agency. The different national agencies are:

Iceland:	“Data Protection Authority”	http://www.personuvernd.is
Sweden:	“The Data Inspection Board“	http://www.datainspektionen.se/
Denmark	“The Danish Data Protection Agency”	http://www.datatilsynet.dk
Finland:	“The Data Protection Ombudsmann”	http://www.tietosuoja.fi/1560.htm
Norway:	“The Data Inspectorate“	http://www.datatilsynet.no

8.0 Practical questions – Privacy legislation applied on the NEEDS project.

8.1 The legal grounds for processing

As described above, one needs legal grounds for processing personal data. Furthermore, one needs legal grounds for transferring personal data to third countries. An important point to make here is that this should be the same legal grounds. Not out of legal necessities, but practical ones.

Where one finds a legal grounds in the Directive Art. 7, one should be aware that if one cannot transfer personal data to third countries without consent, there may not be any reasons not to use consent as the grounds for the processing as a whole. This since the practical work of collecting it has to be done anyway.

8.2 Alternatives and actions

The first action that should be taken, is the specification of what processing one wishes to do, and most importantly, the purpose that is the basis for this processing. Almost every assessment or weighing of considerations and pros or cons will have its base in this purpose.

Secondly, one needs to find a legitimate grounds for processing after Art. 7. The point here is that often there can be several different one can choose to invoke. Each grounds with different advantages and disadvantages. Consent is as described above the preferred grounds for processing from the legislators. This can be seen in the system of the law; with consent one can more or less do whatever one wants. Of course consent is also the grounds that require the largest amount of work. In addition it has the large disadvantage that one can't really be sure that one receives it from everyone. In a project like NEEDS, having a complete directory is important. This is not very likely if one chooses to use consent, because some percentage will always deny consent.

The NEEDS project covers a situation where the listings in the directory will be of individuals either employed by or studying at different Nordic Universities. Among these, the employees seem to be much more important than the students. For internal use, the students e-mail addresses will be available to the institution anyway. For being a part of the directory, it is not evident whether other grounds than consent will be applicable for students.

For employees the grounds for processing can be found through the right the institutions as employers have to decide what is necessary. This is fine if the institution chooses to feel that having all employees in the directory is important to them.

The legal grounds would then be Art. 7 alt. (f)¹³ (or (e)). One should think carefully through how one wishes to use authority before doing this.

In the earlier legislations there were the possibilities to gain consent from the employees organisations. This is no longer possible¹⁴. At the same time an agreement with the same parts that signifies that both employer and employee-organizations support the processing will help establish the fact that the grounds in Art. 7 (f) are applicable, and as such the interests of the controller outweigh the data subjects.

8.3 Organizational questions

As stated earlier, the Controller is responsible for undertaking the duties the law provides. In the NEEDS project, who the controller is may vary, depending on how one chooses to organize it.

The overlaying structure of search engines and mirrors is owned and controlled by someone else than the individual universities, namely UNINETT/SUNET/FUNET. The controller is the body that determines the purpose of the processing of personal data and which means are to be used, and for whom the personal data file is set up. If control over the directory (or mirrors of these) are given to UNINETT/SUNET/FUNET, then they will be controllers according to the law. If UNINETT/SUNET/FUNET performs services for the different universities, they will be “processors”.

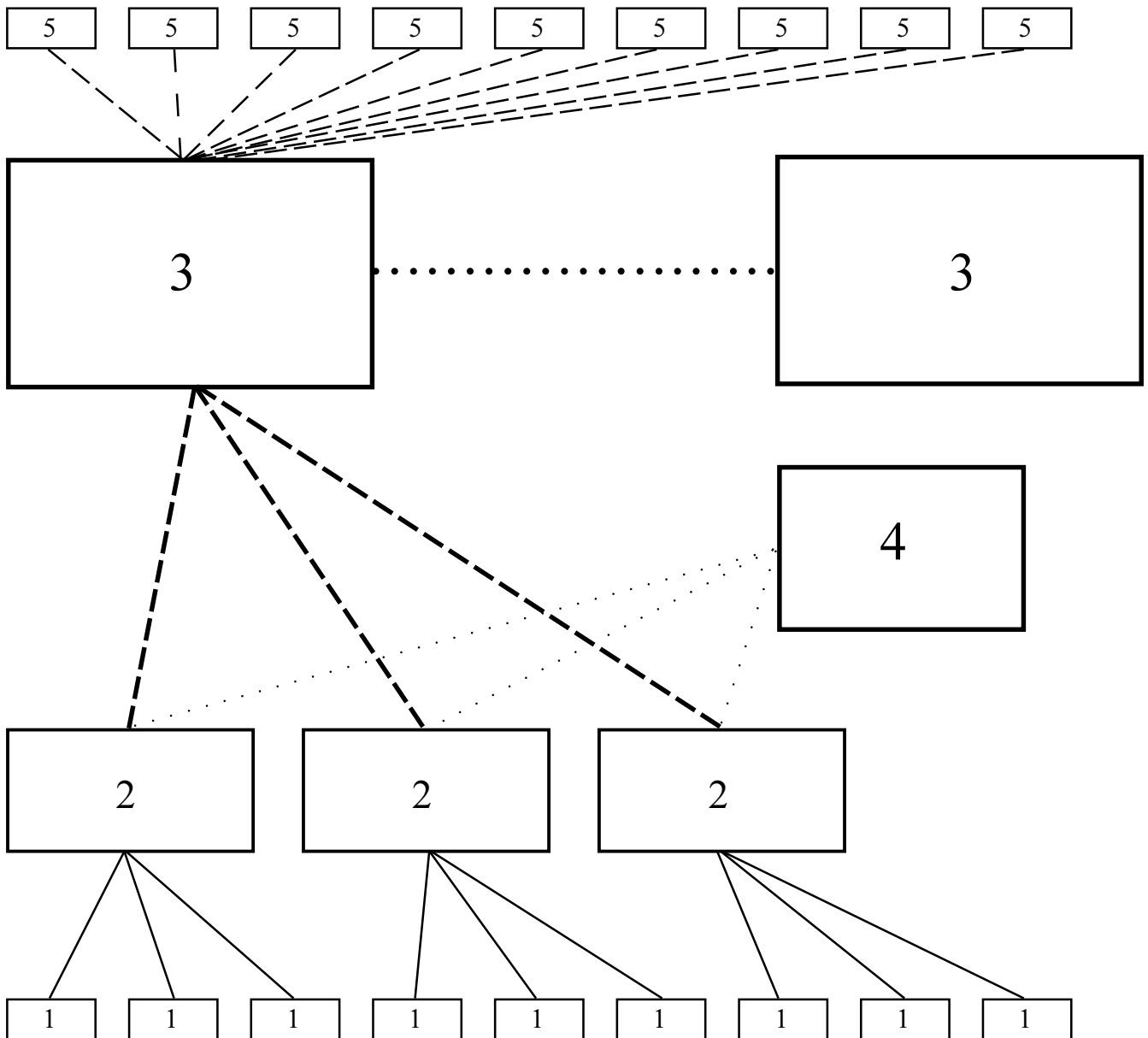
Being the controller is not only something that demands a lot of work, the sending of notifications, the production of documentation etc. It is also important since it is the controller that will have to have a legal grounds for processing. Whils the University of Oslo can demand from its employees that they be included in the directory, UNINETT has no such contractual relationship with the registerd individuals. It is therefore much simpler for the universities to fill the role of the controller than for UNINETT/SUNET/FUNET to do this.

8.4 An organizational model:

A model for organizing the NEEDS project should have the following attributes and be based on the following principles:

- The participating educational institutions are the owners and controllers of their directories.
- The educational institutions, as the controllers and owners of each directory are responsible for securing that the processing of personal data is in accordance with the applicable national law.
- The national education and research networks (UNINETT, SUNET, FUNET) act as processors and service providers on the behalf of the educational institutions.
- The educational institutions grant rights to access, to copy, to distribute and responsibility for providing a specific services such as updating and publication to the national education and research networks via a contract.
- The national education and research networks grant rights to access, to copy, to distribute and responsibility for providing a specific services such as updating and publication between themselves via a contract. The authority to do this is derogated from powers they gain via contracts with the educational institutions.
- All agreements should be based on a common platform of principles/codes of conduct, and then adapted to any special national legislation.
- A site containing common information regarding NEEDS and privacy protection should be available at all bodys involved.

- Any and all contact with the registered individuals shall be between these and the educational institutions they belong to.
- Any and all contact with the national data protection agencies shall be between these and the educational institutions, as far as is possible.



1. Registered individual
2. Educational institution
3. National educational and research network
4. National data protection agency
5. End user.

— Grounds for processing, information about processing, access to personal data, objections toward processing.

— — Contract regulating access etc., the providing of directory data and updating of this.

· · · Notification, inquiries about the processing.

• • • Contract regulation mirroring and shared services, mirroring of sites.

— — Search and result of search in directory.

9.0 A procedure for handling the problem.

9.1 Getting an overview.

The first thing one has to examine, is what the situation is at present and what one wishes to change. If one already has a directory service, one needs to find on what grounds this is processed. Most probably this will be based on an old and no longer valid law. Perhaps (as one had at The University of Oslo) one has gained consent through an agreement with the employees organizations, something which is no longer valid.

In any case one has to make a plan for the process, and the basis of this plan will be the situation at present.

9.2 Parts.

The second thing to examine is who will be involved in the process. The institution, acting as the controller, is obviously taking part in the process, but which individuals within the institution this is, is less certain. Also one should assess the possibility of how one wishes to include the employees organizations in the process. Before one goes outside the institution, and starts interacting with other entities, one should have a clear and jointly shared idea of common goals within the institution.

9.3 Purpose and details of the project.

The stating of a purpose is very important. After the parts within the organization are agreed on a purpose, the rest of the project will be made, according to this purpose. Then a technical and an organizational overview of the project will have to be made. Here a lot can be found through the NEEDS project. Still it is the responsibility of each entity to secure that their insight and documentation is sufficient. When making f.in. a risk analysis, this will have to be based on the individual circumstances in that institution, as well as the overlaying structures of the NEEDS project.

9.4 Legal matters

The legal basis of the project, as this paper examines, should be carefully considered by each entity, in awareness that the responsibility of a processor rests upon them alone. It is important to remember that the National Data Protection Agencies are there to help and guide. These should be used as a resource whenever necessary.

Then gaining consent, or just sending out information (notification will of course have to be done anyway, but if one sends out a written request for consent, this can be included here) to the registered individuals can start. Notification to the National Data Protection Agencies will have to be sent within the time limits stated by the law.

9.5 Checklist

A checklist of elements that have to be in place:

- -no processing based on old laws or agreements that are no longer valid
- -a stated purpose
- -documentaion about the processing, security and risk assessments
- -routines for checking that things are in order,
- -routines for handeling dutys from processing personal data
- -grounds for processing, f.in. statements of consent
- -a recipt from the Dataprotection Agency that one has sent in notification.
- -agreements with the National Reasearch Networks

10.0 Bibliography

Finland:

”Personal Data Act” (523/1999)

Norway:

”Personal Data Act” (14/04/2000 Nr. 31)

”Forskrift til Personopplysningsloven“ 15. desember 2000

”Ot prp nr 92 (1998-99) Om lov om behandling av personopplysninger (personopplysningsloven)”

” NORGES OFFENTLIGE UTREDNINGER NOU 1997: 19

Et bedre personvern - forslag til lov om behandling av personopplysninger”

”Personopplysningsloven - Kommentartutgave”

Wiik Johansen, Kaspersen and Bergseng Skullerud - Universitetsforlaget 2001

Denmark:

“Act on Processing of Personal Data” - (5/10/2000)

Sweden:

“Personal Data Act” (1998:204)

Iceland:

“Act on the Protection of Individuals with regard to the Processing of Personal Data” No. 77/2000

EU:

Directive 95/46/EC

11.0 Endnotes

¹ The term "...or the members of his/her family or household"

² Directive Art. 6, similar terms in the national legislations.

³ Finland: Chapter 7., Sweden: Sec. 30-32, Demark: Title IV, part 11, Norway: §§13, 14.

⁴ Because this was not originally an alternate condition, but an exemption in the Directive.

⁵ Art. 8 nr. 7

⁶ §11, (2) nr. 3: "the processing is carried out for scientific or statistical purposes or if it is a matter of disclosing a civil registration number where such disclosure is a natural element of the ordinary operation of companies, etc. of the type mentioned and the disclosure is of decisive importance for an unambiguous identification of the data subject or the disclosure was demanded by an official authority.

⁷ "Betaling for private dataansvarliges skriftlige meddelelser om indsigt "(Bek. nr. 533 af 15. juni 2000)

⁸ See the Danish law concerning CPR § 29. The CPR is the central register of Persons in Denmark.

⁹ Countries outside the European Economic Area, i.o.w. the EU, Iceland, Liechtenstein and Norway.

¹⁰ § 29 og the Norwegian Law

¹¹ From OT.Prp. 92 1998-99, Chapter. 10.5: "Hvis man i henhold til vilkårene i de almindelige behandlingsreglene har adgang til å utlevere personopplysninger til en ubestemt krets av personer, vil opplysningene uten videre kunne overføres til og offentliggjøres i land som har et tilstrekkelig beskyttelsesnivå for personopplysninger. I slike tilfeller bør det som hovedregel også være adgang til å offentliggjøre opplysningene f eks på en hjemmeside på internett, selv om dette innebærer at personopplysningene blir tilgjengelige også i andre land. Har man først tillatt en vid og i prinsippet ubegrenset spredning av personopplysningene i henhold til de alminnelige behandlingsreglene, kan det neppe hevdes å utgjøre noen trussel mot privatlivets fred å offentliggjøre de samme opplysningene i en global sammenheng. I slike tilfeller bør det derfor ved vurderingen etter § 29 annet ledd i lovforslaget legges avgjørende vekt på det forhold at opplysningene i utgangspunktet kan offentliggjøres til en ubegrenset krets av mottakere. Ved vurderingen av om og i hvilken utstrekning det er adgang til å utlevere personopplysninger i henhold til de alminnelige behandlingsreglene i §§ 8 og 9, må man til gjengjeld ta i betraktning det forhold at man gjennom internett vil få en global spredning av opplysningene. Begrensningene i adgangen til å overføre personopplysninger til utlandet vil etter dette først og fremst få selvstendig betydning for personopplysninger som i henhold til de alminnelige behandlingsreglene bare kan utleveres til en begrenset krets av mottakere."

¹² Personuppgifter och Internet, http://www.datainspektionen.se/kunskapsbanken/notiser_och_press/notiser/2000/oktober2000/2000-10-17.shtml

¹³ Sweden: Sec 10 alt. (f) (or alt (d)), Denmark: Sec. 6 alt (7) (or alt (5)), Norway Sec. 8 alt (f) (or alt. (d)), Iceland: Sec. 8 alt (7) (or alt (5)), Finland: Sec. 8 alt (5) or (8).

¹⁴ Art. 2 (h)

12 Appendices

i: draft of agreement between university and national research network

ii: draft of agreement between two national research networks

i:

Agreement concerning the access to and usage of personal data about employees and students of the University of Oslo in electronic directory services.

This agreement exists between the University of Oslo (UiO) and Uninett (UN).

1.0 Scope

1.1 This agreement regulates the access to and usage of information about employees and students of the University of Oslo in electronic directory services, between the above parts.

1.2 This agreement covers all usage of such information, at all times.

1.3 This agreement exists between UiO as a controller and UN as a processor in the sense these terms are given in the Personal Data Act.

2.0 Dutys of The University of Oslo

2.1 UiO shall provide UN access to the data through a secure connection. UiO shall ensure that the data supplied is as correct as is possible, using reasonable resources.

2.2 UiO shall provide information that is updated every working day. The information source to which UN has access shall be updated as frequently as UiO's directory is.

3.0 Dutys of Uninett

3.1 UN collects data through a secure connection provided by UiO. The information shall be collected, and UN's data updated at least once every working day.

3.2 UN shall provide the directory service to end users without prejudice, without charge and at all times of day.

3.3 UN shall send a report log to UiO stating when it's index server has collected and updated its information concerning UiO every three months.

4.0 Liability and damages

4.1 Any liability for providing access to information shall be minimized by the clear informing of any and all end users, that neither UN or UiO will guarantee, or be held responsible for the accuracy or correctness of the data.

4.2 Any and all liability for the providing of uncorrect information where this information is available updated and corrected from UiO, will be on the part of UN.

5.0 Forwarding data.

5.1 UN can forward, exchange or mirror information from UiO only to national research networks that shall use the information solely for purposes relating to the NEEDS project.

5.2 To perform such an action, UN shall provide that it through contractual means has acquired the right to retract already given information, should the grounds for giving it (powers derived from UiO) vanish.

5.3 Whenever UN wishes to forward, exchange or mirror its information, notice shall be given to UiO at least 14 days in advance.

5.4 Given such notice as described in 5.2, UiO can, for any reason, deny UN the ability to do this.

5.5 If UN has forwarded, exchanged or mirrored information, UiO can at any time, for any given reason, demand this to be stopped, and for UN to retract any given information.

6.0 Security issues

6.1 All handling, publishing and processing of information must be done in accordance with the provisions in appendix a.

7.0 Alterations of the agreement

7.1 Alterations in this agreement shall be made with regard to other agreements between UN and other controllers concerning the NEEDS project.

8.0 The duration of the agreement, termination of the agreement.

8.1 This agreement can at any time be terminated by any of the two parties, with three months written notice.

Appendix A: Risk and Security evaluation concerning the NEEDS project.

ii:

Agreement concerning the access to and usage of electronic directory service data.

This agreement exists between Anet (AN) and Bnet (BN).

1.0 Scope

1.1 This agreement regulates the access to and usage of electronic directory service data between the above parts.

1.2 This agreement covers all usage of such information, at all times.

1.3 This agreement exists between AN and BN within the limits of their ability to exchange such data, as granted them by agreement with the owners of that data.

1.4 This agreement exists between AN and BN as equal parts, where both AN and BN fill the roles as both supplier and recipient of data at the same time. The rights and duties of a part by filling one of these roles shall not influence the rights and duties of that part relating to its other role.

2.0 Dutys of the supplier of data

2.1 The supplier shall provide the recipient access to their data through a secure connection.

2.2 The supplier shall provide information that is updated once every working day from the original source.

3.0 Dutys of the recipient of data

3.1 The recipient collects data through a secure connection provided by the supplier. The information shall be collected, and the recipients data updated at least once every working day.

3.2 The recipient shall provide the directory service to end users without prejudice, without charge and at all times of day.

3.3 The recipient shall, every three months, send a report log to the supplier stating when it's index server has collected and updated its information from the supplier.

4.0 Liability and damages

4.1 Any liability for providing access to information shall be minimized by the clear informing of any and all

end users, no part in this agreement, or their sources of data will guarantee or be held responsible for the accuracy or correctness of the data.

5.0 Forwarding information

5.1 The supplier can forward, exchange or mirror information from its sources only to a recipient that shall use the information solely for purposes relating to the NEEDS project.

5.2 To perform such an action, The supplier must have been given the power to do this, in an agreement with the owner of the data. If, at any time this power is retracted, any and all data that has been given based on this shall be returned or deleted.

5.3 The data given through this agreement shall not be forwarded, copied or mirrored to any other entity or organization.

6.0 Security issues

6.1 All handling, publishing and processing of information must be done in accordance with the provisions in appendix a.

7.0 Alterations of the agreement

7.1 Alterations in this agreement shall be made with regard to other agreements concerning the NEEDS project.

8.0 The duration of the agreement, termination of the agreement.

8.1 This agreement can at any time be terminated by any of the two parties, with three months written notice.

*Appendix A: Risk and Security evaluation concerning the NEEDS project.
(Not yet present)*

13 Legal Texts

The directive 95/46/EC (official english translation):

http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

Norwegian law (nnoofficial english translation):

<http://www.datatilsynet.no/lov/loven/poleng.html>

Swedish law (unofficial english translation):

http://www.datainspektionen.se/in_english/legislation/data.shtml

Danish law (unofficial english translation):

http://www.datatilsynet.dk/include/show.article.asp?art_id=443&sub_url=/lovgivning/indhold.asp&nodate=1

Icelandic law (unofficial english translation):

<http://www.personuvernd.is/tolvunefnd.nsf/pages/1E685B166D04084D00256922004744AE>

Finnish law (unofficial english translation):

<http://www.tietosuoja.fi/uploads/hopxtvf.HTM>