Data Service Infrastructure for the Social Sciences and Humanities

EC FP7

Grant Agreement Number: 283646

Deliverable Report

Deliverable: D6.5
Deliverable Name: Handbook on legal and ethical issues for SSH data in Europe, Part II
Deadline: 31st December 2014
Nature: O

Responsible: NSD, UiB
Work Package Leader: MEA (MPG)

Contributing Partners and Editors:
Marianne Bøe (NSD), Linn-Merethe Rød (NSD), Carla Parra (UiB), Koenraad De Smedt (UiB), Vigdis Kvalheim (NSD), Katrine Utaaker Segadal (NSD), Trond Kvamme (NSD), Bamba Dione (UiB), Gunn Inger Lyse Samdal (UiB),

Part II

Handbook in legal and ethical issues for SSH data in Europe

1. Introduction

The use of research data is often restricted by a set of legal regulations and ethical guidelines. Researchers working with data must know the possible legal restrictions that apply to research data, and the potential ethical issues in handling data. The present handbook intends to be a concise introduction to some legal and ethical aspects of working with research data in the Social Sciences and Humanities.

The handbook will present issues related to the legal and ethical regulations relevant for the use of personal data in research. Moreover, it will deal with copyright issues, as well as the ongoing debate connected to the draft of a new general EU data protection regulation. The handbook will provide an overview of these issues in relation to the various process steps in research projects, from preparation and design, to the preservation and the access and reuse of personal data for research purposes.

Currently, personal data in the European Union is protected by domestic implementations of the Data Protection Directive (95/46/EC). The challenges of the Directive from a research perspective are the different ways that each EU country implements or practices the law, and how this has led to an uneven level of data protection and an uneven level of access to individual data for scientific purposes, seriously impeding cross country research.

Consistent with the advisory nature of an EU directive, the member state data laws vary widely. In addition, all member states have established their own unique Data Protection Authorities, compliance structures, notification and approval processes, and other bureaucratic or regulative procedures. In particular, the variations of definitions of personal data, anonymisation and the requirements for legal approval provide different preconditions for the kind of research that is allowed within each country. While some laws offer data subjects at least the Directive's core protections, some add extra rights with regard to e.g. the use of encrypted or de-identified data, requirements for consent and access to data.

The legal variations, combined with new technological developments and an increase in the amount of personal data that is being collected and processed across Europe, pose new challenges. As a result, the demand for a new coherent general data protection regulation has come to the fore. The need for a consistent legal framework across Europe is one important reason why the EU is currently upgrading the data protection regulation from directive to

law. Thus the proposal for a new General Data Protection Regulation (GDPR) and the subsequent practice at the national level is of great interest to the scientific communities and research infrastructures in Europe.

2. Privacy and Data Protection

2.1 Introduction

The regulations on the processing of personal data affect large areas of the research in the SSH domain. Currently, the processing of personal data in the European Union is regulated by domestic implementations of the Data Protection Directive (95/46/EC). These implementations vary widely across borders, as will be discussed further in chapter five. Due to the inconsistencies and contradictions of the member states data protection regulations, the demand for harmonisation of rules and practices is high.

The need for a consistent legal framework across Europe is one important reason why the EU is currently upgrading the data protection regulation from directive to law. A regulation is a binding legislative act and must be applied in its entirety across the EU. Directives lay down certain results that must be achieved by all member state, but the individual country is free to decide how to transpose directives into national laws.

The proposal for a new General Data Protection Regulation (GDPR) and the subsequent practice at the national level is of great interest to the scientific communities and research infrastructures in Europe. One important concern is whether the new regulation creates good, secure and predictable framework conditions for scientific research and research infrastructures.

2.2 The new General Data Protection Regulation (GDPR)

In January 2012 The European Commission proposed a comprehensive reform of the EU's 1995 data protection rules. The main policy objectives for the Commission are to:

- "Modernise the EU legal system for the protection of personal data, in particular to meet the challenges resulting from globalisation and the use of new technologies;

- Strengthen individuals' rights, and at the same time reduce administrative formalities to ensure a free flow of personal data within the EU and beyond;

- Improve the clarity and coherence of the EU rules for personal data protection and achieve a consistent and effective implementation and application of the fundamental right to the protection of personal data in all areas of the Union's activities" (http://ec.europa.eu/justice/data-protection/review/index_en.htm)

The Commission's proposal for a new General Data Protection Regulation (GDPR) did not signify any dramatic changes in the legal framework for the research community. It included more or less all of the research provisions implemented in the current Data Protection Directive.

However, one very important research provision had been removed from the wording of the Commission's proposed regulation. Article 6 (b) of the Directive states that the processing of personal data for historical, statistical or scientific purposes is not considered to be incompatible with the original purpose of collecting the data. In the proposed GDPR (Article 5 (b)), this provision is now removed from the text of the law and included in recital (40) of the preamble. This might potentially weaken the position of research, as this exemption is seen as a basic principle and a guarantee for further (secondary) use of personal data for scientific purposes regardless of the original purpose (Kvalheim, 2014).

In December the same year, the main rapporteur for the GDPR in the EU Parliament, Jan Philipp Albrecht, issued a draft report on the GDPR for the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee). This report proposed several amendments to the Commission's proposal, and has been subject to extensive discussion. Especially in the health science communities in Europe, the amendments were a source of widespread concern as they put severe restrictions on the processing and preservation of research data. The Albrecht Report proposed to delete several research exemptions that initially had been included in the Data Protection Directive 95/46/EC (and were continued in the proposal from the Commission to ensure a balance between research interests and protection of personal privacy). This is justified by arguing that scientific research is not special with regard to its public interest, and do not deserve a privileged position within the

legal framework: “Processing of sensitive data for historical, statistical and scientific research purposes is not as urgent or compelling as public health or social protection. Consequently, there is no need to introduce an exception which would put them on the same level as the other listed justifications” (Amendment 27). The removed provisions are essential for the possibility of reusing and sharing research data, and for the long-term storage and open access to data.

Based on input and draft opinions from stakeholders and other committees in the EU Parliament, on October 22, 2013, the LIBE committee voted to approve a new compromise Draft Regulation. On March 12, 2014, the European Parliament accepted the proposal, including the amendments proposed by the LIBE Committee, by voting in plenary.

On one hand, the proposed GDPR adopted by the Parliament does not involve as dramatic consequences for research as feared when the Albrecht Report was issued. Important exemption provisions for research that are included in the Data Protection Directive 95/46/EC are continued in this proposal: Processing of personal data which is necessary for research purposes shall be lawful without consent subject to certain safeguards, cf. Article 6 second paragraph. This exemption also regards sensitive personal data, cf. Article 9 second paragraph (i). In addition, exemptions from the obligation to provide information (cf. Article 14 5 (b)), the obligation to erase (cf. Article 5 (e)) and the right to be forgotten (cf. Article 17 3 (c)) are included, all of which apply specifically to research. Moreover, new and separate provisions have been included for the processing of personal data by archive services, in which storage for research purposes is specifically mentioned, cf. Article 9 (ia). This strengthens the legal framework conditions for research infrastructures and research data archives.

On the other hand, several amendments to the EU Commission's proposal made by the Parliament may have negative consequences for specific types of research. First and foremost, the essential principle stating that research is a „not incompatible purpose“ as mentioned above, has now been removed entirely from the GDPR. “This means that the basic guarantee for further use of data for research purposes regardless of why the data were initially collected is lost and that the special position afforded research as a particular legitimate public interest is weakened in the proposed data protection legislation. This can, in the worst-case scenario, lead to a limitation on secondary use of data for research purposes, especially when the possibility of granting exemptions from the requirement for explicit consent for research purposes has also been more restricted” (Kvalheim 2014).

Moreover, the Parliament's proposal include a number of other provisions that may make conditions more difficult for research: It is a requirement that consent must be limited to one or more specified purposes, cf. Article 6 first paragraph (a), cf. Article 9 second paragraph (a) and cf. Article 7 fourth paragraph. This might entail that broad consent is not an option. The general condition that data for research must be pseudonymised has been tightened in the proposed regulation; cf. Article 83 (b). This primarily concerns projects that are not based on specific consent, and may lead to a significant tightening of the conditions for research.

In research projects where health data are processed, the main rule is that consent from the data subject is required cf. Article 81 (2). Furthermore, the pseudonymisation requirement for the processing of health data for research purposes applies in all cases, even when the processing is based on consent. Exemptions from the consent requirement for processing of health data may be granted for research that serves a high public interest, but it is up the individual Member State to adopt such an exemption provision in national law, cf. Article 81 (2a). As a consequence the GDPR might tighten the conditions for processing of health data for research purposes, and does not secure harmonisation of the legal framework in this area.

However, if the final regulation is in line with the Parliament's proposal, the GDPR probably will reduce the fragmentation of data protection laws across Europe. Beyond this, the improvement of the legal framework conditions within the SSH research domain are limited. There is a clear tendency in this proposal towards strengthening the right to personal privacy and control of own personal data at the expense of researchers access to such data.

There is still some uncertainty connected to the further processing of the GDPR. To become law the proposed Regulation has to be adopted by the Council of Ministers using the "ordinary legislative procedure" (co-decision). The Parliament, the Council and the European Commission have to agree on the final text through a trilogue. Following the trilogue, the proposed Regulation will be put to a vote of the Parliament and, if adopted, there will be a final implementation period before the Regulation comes into force in the EU Member States.

A joint Statement by Vice-President Andrus Ansip and Commissioner Věra Jourová on European Data Protection Day, 28 January 2015 confirms that that the proposal is still being discussed by the two European Union co-legislators, the European Parliament and the Council. Justice Ministers from the Member States have been negotiating on various aspects of the data protection regulation to reach a common agreement on its provisions among

Member States. However, apparently the discussion on how to protect the scientific use of personal information within the new legal framework is still on-going.

3. Intellectual Property Rights and Copyright

3.1 Introduction

A researcher's possibilities to use and cite data are determined by who owns the data and what are the rights to their exploitation. Therefore, Intellectual Property Rights (IPR) and Copyright must not be overlooked in the collection, archiving, dissemination and re-use of research data. The applicable conditions in each case may vary depending on national and international legislations, as well as private agreements, such as the work agreement between researchers and their employers. All parties shall take copyright and licensing conditions into account: researchers and their employers, repositories and users.

Despite general guidelines on IPR issues that are at the disposal of researchers,[1] the situation is often complicated. Some data sets consist of many parts and layers which are associated with different owners and different rights. Annotated language data, for instance, consist of text, spoken, or multimodal corpora, which, for study purposes, are enriched by means of transcription, translation, alignment, part-of-speech tagging, parsing or other linguistic analysis. Although annotators may claim ownership to the annotations, the original source texts are often published works of fiction or non-fiction, to which their authors or publishers claim copyright. Thus, it may be necessary to obtain permission to both the source texts and the annotations, in order to effectively investigate and cite certain works with digital means, and to preserve research data which includes copyrighted works.

Copyright has different expiration dates in different countries, such that works may enter into the public domain at different times. Several factors determine whether a work may be considered to be in the public domain, and sometimes the expiration dates also depend on the nature of the work. For instance, sometimes a distinction between written texts or videos is established. It may also be the case that a work has entered the public domain, but it has been

[1] The "OECD Principles and Guidelines for Access to Research Data from Public Funding" are an example of these.

newly released in some other form (e.g. a critical edition of a classic work, or a new version of a piece of music), which subsequently has acquired some Intellectual Property Rights (IPR) which must be complied with. Therefore, prior to using any work, the national legislation of the country where such work was originated has to be consulted. EU Law, for instance, establishes that copyright expires 70 years after the death of the copyright owner.

In order to use copyrighted works (copying, adapting, sharing, processing, etc.), the permission of the copyright owner shall be obtained. This may prove to be challenging, especially when dealing with complex copyright works.

Whether and under which conditions researchers may be entitled to make copies of copyrighted works for research purposes depends on the country. Most countries are signatories of the Berne Convention,[2] which requires them to recognise the copyright of works of authors from other signatory countries. However, the extent of copyright as well as possible exceptions, often under the headings "fair use" or "fair dealing", depend on national legislation.

The United States of America has a judicially established practice of "fair use" that makes it legal to make copies of copyrighted works without explicitly obtaining permission from the right holders.

In Norway, the regulations to the Copyright Act §1-4 establish that the Ministry of Culture can grant research institutions the right to access and use copyrighted texts for research purposes.

EU law also establishes some exceptions for re-use of copyrighted works that *can be implemented* within Member States (i.e. the laws are country-dependent). Such exceptions are:

- Criticism and review
- News reporting
- Private copying
- Parody

[2] The "International Convention for the Protection of Literary and Artistic Works", commonly known as the Berne Convention, is an international copyright agreement under which all contracting countries provide protection to those works published in the signatory countries, as well as to unpublished works by citizens of residents of such countries.

- Research
- Education
- Archiving and preservation

As copyright is currently country-dependent under EU copyright law, the laws of all countries of origin of the different sources of data are to be respected. Thus, depending on the country of origin, different uses may be allowed and different restrictions may apply.

The United Kingdom has partially implemented some of the exceptions that EU law allows its member states to implement. On 1 June 2014, several new regulations came into force. These regulations include provisions as regards disability, research, education, libraries and archives, and public administration. With regard to research, the new regulations allow the usage of all copyright works for research, provided this usage can be considered "fair".[3]

3.2 The European reform

Europe does not have a unified legal framework for copyright, but there are different legal frameworks in the various European countries. These differences create barriers for cooperative R&D across borders within Europe, in particular for text and data mining. Digital materials and services pose new challenges to the interpretation of copyright legislation and Europe has no provision for *fair use* of materials protected by copyright.

On 5 December 2013, the European Commission launched a public consultation as part of its on-going efforts to review and modernise the EU copyright rules. A consultation document with questions was made available and all stakeholders were welcome to contribute to this consultation, which closed on 5 March 2014. The number of responses was 9599.

In July 2014, a consultation report summarising the responses received was published by the EU.[4] In it, several issues as regards copyright are raised. With regard to research, the focus was on access to scientific publications and scholarly articles. However, there were specific questions as regards text and data mining.

[3] "Fair dealing" is defined in the new regulations as the usage a fair-minded and honest person would do with the work.
[4] http://ec.europa.eu/internal_market/consultations/2013/copyright-rules/docs/contributions/consultation-report_en.pdf

As pointed out in the consultation report, there is a general dissatisfaction regarding the current situation among researchers and institutional users. Researchers "highlight that text and data mining is a fundamental tool for research and consider that, at present, Europe is missing out on the benefits that text and data mining can bring to competitiveness and innovation and to citizens. They put forward two main categories of obstacles to text and data mining: legal uncertainty on whether and how copyright may apply to text and data mining and problems with existing licensing mechanisms, which they generally consider inadequate" (EC, 2014, p.63).

In the report it is also mentioned that some respondents "consider that text and data mining is easier in non-EU countries that have "fair use" provisions in their legal systems. According to them, this gives North American universities a competitive advantage over universities and companies based in the EU". The same was raised by one Member State, who highlighted "the need to make sure that European researchers are not at a competitive disadvantage internationally" (EC, 2014, p.67). Moreover, many Member States recognised "the benefit that text and data mining can offer to scientific research" (EC, 2014, p. 67).

Researchers and institutional users argue that licenses are not an appropriate solution for purposes of text and data mining, but rather constitute a barrier and a source of transaction costs. Authors and publishers, on the other hand, think that the current licensing solutions are appropriate.

Taking into account the responses gathered to the consultation, the EU is planning a copyright reform. Although some have argued against a research exception for text and data mining, the arguments in favour of it, summarised in the report, may indicate that the reform may include an exception for research purposes. It also seems that the reform will also try to establish a more homogeneous arena as regards copyright for all Member States. This would imply that the same regulations would be applicable in all EU countries, thus simplifying the current situation, in which laws for each Member State participating in a project, or being the source of data have to be considered.

3.3 Licensing schemes

To the extent that research data may contain materials which are not in the public domain and no lawful exception applies, permission needs to be obtained to copy, preserve and distribute the data. For data deposited in repositories, various parties are usually involved, so that in general, two main agreements are required:

1. A Deposition License Agreement (DELA) is an agreement between the *repository* and the *owners* of the rights to a deposited resource. It regulates the conditions under which the resource will be made available. As part of these conditions, it specifies which EULA (see below) will be applied.
2. An End User License Agreement (EULA) is an agreement between the *repository* and the end *users* of a deposited resource. It regulates the conditions under which the users can access and exploit the resource. Terms of use which are not specific to a particular resource, but which apply for all repository services, are brought together in the Terms of Service agreement (TOS).

By *license*, in this context, one usually means the conditions set forth in the EULA. Deliverable D 4.5.1[5] of the QT LaunchPad project [Tsiavos et. al.: 2014, pp. 21-27] offers a good overview of the types of licenses currently available. The widely known and used Creative Commons[6] licenses are standard licenses which cannot be modified. They enable quick and easy licensing of resources. In contrast, there also exist license templates which can be modified according to specific needs that arise in negotiations.

Generally, all licenses establish conditions regarding the attribution of the resource, whether or not the resource may be used for commercial purposes, whether or not derivate works are allowed, and the limitations on the kind of use that can be done with the resource.

Three main types of licenses may be distinguished:

- Public licenses, which allow everyone to use the resource for whichever purpose.
- Academic licenses, which allow users of academic institutions to use the resource and are more restrictive.
- Restricted licenses, which establish certain requisites to grant access to the resource to potential licensees and also establish restrictions on the kinds of use that may be done.

[5] http://www.qt21.eu/launchpad/system/files/deliverables/QTLP-Deliverable-4_5_1_0.pdf
[6] http://creativecommons.org/

Sometimes repositories offer prepared licenses with the aim of facilitating the licensing of resources. In that case, several templates are provided, and the researcher agrees the kind of license for their resource in cooperation with the repository. If required, the template is modified to include all additional terms, not previously foreseen in the template, that need to be observed. In turn, repositories safeward that end users agree with the terms established in the license.

An essential component for enforcing end user license agreements is the user authentication and authorisation process prior to accessing data. A proper authentication and authorisation infrastructure (AAI) ensures that only users with the appropriate credentials get access to copyrighted data. Users are also required to read and accept license agreements where all provisions regulating the usage of such data are specified. By accepting the terms of the licenses, users commit to abide by those terms. Click-through licenses require a high level of trust based on a secure AAI (see also the DASISH training module on AAI).

3.4 IPR issues: conclusion

The primary IPR bottleneck for access to materials in the Humanities is copyright. The current lack of a uniform European copyright law including exceptions for research poses a challenge for researchers working with copyrighted data. Copyright clearing can be very bothersome, not only because many rights holders may be involved, but also because the laws of all countries where the copyrighted data were originated must be taken into account. With the upcoming EU Copyright reform, this situation may change and facilitate researchers' access and (re-)use of data.

Before using data for research or releasing a new resource, researchers have to ensure that this does not violate any laws regarding IPR issues and copyright. Additionally, upon the release of a resource, it is advisable to provide it with an appropriate license that ensures the rights and limitations provided to end users.

3.5 Further readings

CLARA Association (2011). The Management of Copyright in Norway. Retrieved 23 June 2014, from: http://www.clara.no/dokumenter/clara-brochure.pdf

CLARIN (2014). CLARIN's vision on the EU copyright reform. Retrieved 23 June 2014, from: http://www.clarin.eu/sites/default/files/CLARIN-ERIC-EU-consultation-final.pdf

CLARINO (2014). CLARINO's vision on the EU copyright reform.

CORDIS. Guide to Intellectual Property Rules for FP7 projects. Publication date unknown. Retrieved 23 June 2014, from: http://ec.europa.eu/research/participants/data/ref/fp7/89593/ipr_en.pdf

ECS (2014). European Copyright Society Answer to the EC Consultation on the review of the EU copyright rules. Retrieved 23 June 2014, from: http://www.ivir.nl/nieuws/ECS_EC_consultation_copyright.pdf

Hargreaves, Ian (2011). Digital Opportunity: A Review of Intellectual Property and Growth. Retrieved 23 June 2014 from http://www.ipo.gov.uk/ipreview-finalreport.pdf

Intellectual Property Office (UK) (2014). Changes to copyright law and guidance. Retrieved 23 June 2014, from: http://www.ipo.gov.uk/types/hargreaves/hargreaves-copyright/hargreaves-copyright-techreview.htm

Intellectual Property Office (UK) (2014). Exceptions to copyright: Research. Retrieved 23 June 2014, from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/315014/copyright-guidance-research.pdf

Intellectual Property Office (UK) (2014). Explanatory Memorandum on the Draft Statutory Instruments. Retrieved 23 June 2014, from: http://www.legislation.gov.uk/ukdsi/2014/9780111112717/pdfs/ukdsiem_9780111112717_en.pdf

Mannapperuma, Menesha A., Schofield, Brianna L., Yankovsky, Andrea K., Bailey, Lila and Urban, Jennifer M. (US) (2014). Is it in the Public Domain? A handbook for evaluating the copyright status of a work created in the United States between January 1, 1923 and December 31, 1977. Berkeley Law, University of California and Samuelson Law, Technology and Public Policy Clinic. Retrieved 23 June 2014, from: http://www.law.berkeley.edu/files/Final_PublicDomain_Handbook.pdf

UK Government (2013). Enterprise and Regulatory Reform Act 2013. Retrieved 23 June 2014, from: http://www.legislation.gov.uk/ukpga/2013/24/contents/enacted

UK Government (2014). Copyright, Designs and Patents Act 1988. Retrieved 23 June 2014, from; http://www.legislation.gov.uk/ukpga/1988/48

United States Court of Appeals for the Second Circuit (2014). Authors Guild v. HathiTrust Appeal Decision. 11 June 2014. Retrieved 23 June 2014, from: https://www.eff.org/files/2014/06/10/agvhathitrust.pdf

United States District Court Southern District of New York (2013). Authors Guild et al. v. Google. Lawsuit on the case of Google Books. November 2013. Retrieved 23 June 2014, from http://www.wired.com/images_blogs/threatlevel/2013/11/chindecision.pdf

4. Working with private information

In the study of survey and census data, *microdata*, i.e. information at the level of individual respondents, may be perceived as sensitive, as it may collect a person's name, age, home address, educational level, health history, employment status, and many other variables, recorded separately for every person who responds. Furthermore, the metadata of *interviews* and spoken or written language *corpora* may reveal the names and other personal data of participants in the interviews or language corpora. Finally, the audio or text itself of interviews and other spoken or written language data may contain names or describe people in ways that affect their privacy.

4.1 Anonymisation and aggregation

Concerns about data protection of personal privacy can sometimes be eased by anonymising the data. This implies that personal information is removed so that the data can no longer be traced to individuals. At the level of metadata, the names of individuals can be erased or replaced with arbitrary anonymous identifiers.

At the level of spoken or textual data, similar techniques could be applied, i.e. names could be replaced by codes such as <name /> which act as placeholders for names. In some cases anonymisation of named entities may not be sufficient, since spoken or written descriptions of people could still provide enough clues to reveal their identity.

There is, however, no common definition of sufficiently anonymised private information. For instance, in the UK anonymisation is "…the process of turning data into a form which does not identify individuals and where identification is not likely to take place".[7] In Germany, the Federal Data Protection Act states that: "Rendering anonymous means the modification of personal data so that the information concerning personal or material circumstances can no

[7] UK Information Commissioner's Office: What is anonymisation?:

http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual (cf. FDPA, Section 3.6).

Therefore, in many cases, even anonymised data will not be distributed outside of the research group who collected the data. Instead, the data will often be aggregated or statistically processed, and only the results of such processing will be disseminated. At the initial stage of data collection, however, anonymisation will not have been applied. In such cases, it will be necessary to limit access to the data and to provide secure storage and transmission.

Although most informants probably will never read an article in a (foreign) academic journal, the article should anyhow be written as if it would end up in the hands of the informants' friends, neighbours or colleagues. Distance in geography, language and culture is not sufficient to ensure privacy. Dialect expressions in quotes, the participant's age or occupation, information about where the project is carried out, and stories that reveal specific and special incidents are examples of factors that may increase the risk of recognition. Such occasions cannot always be specified in advance in the description of the project. However, they must be considered along the process according to ethical standards. Sometimes it is almost impossible to promise participants' anonymity in the publication of a qualitative study. Although neither persons nor institutions are mentioned by name, participants still could be recognised. This particularly is evident of studies based on a small and distinctive sample, for instance related to a particular place or a particular group of people.

The researcher may also find that the most evident quotes or observational data are so full of recognisability that it is not possible to use them in a publication. If the consequence is that the results would be too poorly documented in the presentation of the findings, it can be tempting to compromise. Compromises that compromise the informants' privacy, however, are not ethically acceptable.

However, publication of identifiable informants doesn't always have to compromise with ethics. Some informants even want to be recognised for their contribution to research. It is anyhow important to recall that such identification cannot be based on the participant's desire alone. The researcher must still take independent responsibility to assess whether this could harm the person in any way.

When e.g. audio and video recordings are published on the Internet, it is obvious that such publication shall be based on informed consent. In addition to obtaining informed consent, the

researcher has a responsibility to make an independent ethical review of possible integrity violations of such publications (The Norwegian National Research Ethics Committees:2010).

The lack of legal harmonisation in data access regimes due to legal uncertainty leaves several unsolved issues for researchers. Gaps, inconsistencies and contradictions may turn up when researchers are involved in cross-country research and data sharing.

Since the adoption of the Directive, a lot has changed in the area of data protection, "…notably technological developments, increased collection and processing of personal data, including for law enforcement purposes, with a patchwork of applicable data protection rules and globalisation of markets and cooperation".[8] The Directive was introduced when the Internet was still in its infancy. Rapid technological developments and subsequent data harvesting techniques ("big data" from e.g. social networking sites, cloud computing, location-based services, smart cards, etc.) have brought new challenges for data protection and anonymisation.

The aim of the recent data protection reform in EU, the new General Data Protection Regulation (GDPR), has been to modernise the principles from the 1995 Data Protection Directive and to strengthen citizens' rights and thereby help restore trust. Better data protection rules are aimed at the EU citizens so that they can be more confident about how their personal data is treated.

4.2 Secure storage and access

When handling sensitive data, special precautions need to be taken in order to avoid breaches of personal data protection. IT systems containing sensitive data must satisfy the criteria set forth in national or international norms for secure systems. Such norms may be legally established for a sector.[9] Secure storage on a server implies that researchers are not allowed to

[8] See explanatory statements in LIBE draft report 2012/0011 (COD) dated December 17, 2012.

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

[9] For the health sector in Norway, for instance: http://www.normen.no

download the data on their own computers; but that the data must be securely kept on a certified server and any processing must be carried out on that server.

Backup and transport of such data must always be encrypted. Access to the data on the server must be tightly controlled. Normally, authentication of users must use a two-factor solution, based on something the user knows (such as a password) and something the user has (such as a mobile phone, smart card or code generator). Most of all, trusted users must be accredited by their departments or personnel managers, who must keep logs which document who has access to what. Users need to be properly educated in matters of legal issues, ethics and security protocols.

Procedures and technologies for secure storage are increasingly being implemented in relevant research environments. They are critical in health related research areas, but also relevant for the social sciences dealing with microdata and interviews, and for language sciences dealing with spontaneous spoken and written language.

5. The implementation of the regulation in member countries

5.1 Introduction

In this chapter, similarities and differences in legal requirements within the following countries will be presented: Germany, Netherlands, Denmark, Iceland, Sweden, Norway, Finland, Spain, UK and Estonia. All countries have implemented the Data Protection Directive (95/46/EC). However, both implementations and interpretations vary widely across Europe. The main topics which will be covered here are regarding authority structures, definitions of personal data, notification and approval processes, conditions regarding preservation and reuse of personal data and copyright issues.

5.2 Preparation and design

5.2.1. Data Protection Authorities, Data Protection Officers and Laws

All the EU-countries have National Data Protection Authorities (cf. the European Commission website). In Appendix II, you will find a list of all such Authorities in Europe.

Germany stands out with regard to the number of authorities and personal data acts. Data protection supervision in Germany is regulated by the Federal Data Protection Act (FDPA), as well as each of the 16 states' own data protection acts. The FDPA mainly deals with the use of data by public bodies that are either part of or influenced by the Federation and any use of data by private persons or enterprises. By contrast, the scope of application of the state Acts is limited to public bodies being part of, or being influenced by, the respective state. By far the majority of research institutions and universities (except some private universities) as well as more or less all public hospitals, are controlled by the state legislation (Kühn 2004).

Each individual German state has a Data Protection Authority which is responsible for the enforcement of data protection laws and competent for the supervision of data controllers established in the relevant state (The Federal Commissioner for Data Protection and Freedom of Information).

The EC 95/46 Directive states that in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided under certain conditions. A data protection official appointed by the controller ensures that the processing carried out is not likely to adversely affect the rights and freedoms of data subjects. The data protection official must be in a position to exercise its functions in complete independence.

The system of appointing a data protection officer is central in many countries, as e.g. also is the case in the relatively new Estonian Personal Data Protection Act from 2008. The Swedish Personal Data Act also incorporates the system of independent data protection officers, appointed by the organisation.

Similarly both Iceland and Norway have data protection officer arrangements. In Norway, exemption from obtaining license from the Supervisory Authority can be given, if the controller has appointed a Data Protection Official,[10] given notice of this to the Data Protection Authority, and the official has recommended the project (cf. Article 7-27 of the Norwegian Data Protection Regulation).

In the German Federal Data Protection Act, it is mandatory to appoint a data protection officer for public and private bodies with more than nine employees processing personal data by automatic means (cf. Section 4f of the FDPA). This makes Germany the only country in our sample whereas personal data officers are mandatory. The German State legislation varies however slightly, whether it is mandatory or not with appointment of officials. Anyhow, all the German universities, research centres and research hospitals have appointed data protection officials (Kühn 2004).

In Iceland, there is no legal requirement to appoint a data protection official. However, the Icelandic Data Protection Authority can handle a case regarding the processing of sensitive personal data by stipulating, that a special data protection official be appointed to oversee, on behalf of the Data Protection Authority that the processing is in compliance with law (jf. Article 35 in the Icelandic DPA).

In the Netherlands, the effect of self-regulation for the different industries or sectors is specially emphasised in the Data Protection Act, and the Dutch Data Protection Authority (College Bescherming Persoonsgegenes (CBP)), promotes the possibility of appointing a data protection officer and also advises different sectors to formulate their own code of conduct (CBP website).

Article 25 of the Dutch DPA states that one or more organisations planning to draw up a code of conduct may request the CBP to declare that the rules contained in the said code properly implements the DPA or other legal provisions on the processing of personal data. Within the research sector, e.g. there are codes of conduct for scientific practice, use of personal data and for medical research.

[10] Norwegian Social Science Data Services is appointed as the Data Protection Official for around 150 Norwegian research and educational institutions: http://www.nsd.uib.no/personvern/en/index.html

The encouragement of drawing up codes of conduct, taking account of the specific features of the various data processing sectors, is further emphasised in Article 38 in the new EU regulation proposal.

In Finland, the system of Authorities and Data Protection Officers is slightly different, whereas the Personal Data Act outlines two separate data protection authorities; the Data Protection Ombudsman and the Data Protection Board. The Ombudsman's duties are among others to supervise that processing of personal data is in accordance with the Act, while the Board deals more with questions of principle relating to the processing of personal data. Further, there is no specific requirement in the Finnish Personal Data Act for organisations to appoint a data protection officer.

The data protection officer arrangement is continued and strengthened under the proposal for new data protection regulations in Europe (Kvalheim 2014).

5.2.2 Definitions of personal data

According to the 95/46/EC Directive, 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" (cf. Article 2, a).

The definition in the proposed regulation is slightly more detailed in its description. However, the intention seems to remain the same:

> "personal data means 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 identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person" (cf. Article 4.2).

The current definition of personal data, and by this, which data actually falls under the scope of law, varies across Germany, Netherlands, the Nordic countries, Spain, UK and Estonia.

One nuance in the definitions is whether the data is to be considered as personal data if the data controller cannot him or herself by possible means identify the data subjects, as e.g. could be the case concerning de-identified data where the data controller doesn't have access to encryption key. Such nuance is however often specified by practice rather than by law. Data is in some countries considered as personal, regardless of the form or format in which the data exists. This is to be considered as a stricter and perhaps more factual implementation of the Directive's definition of personal data.

According to the Dutch Data Protection Act (DPA), personal data is defined as any information relating to an identified or identifiable person (cf. Article 1(a)). As the Act itself leaves it open as to who can identify the data subject, the Guidelines to the Dutch DPA states that:

[Whether a person is identifiable] depends on the possibilities the controller has at his disposal. If actual identification is reasonably excluded because of encryption of the data and/or agreements about the access to the data, the person is not identifiable. The actual situation is always the determining factor (Ministry of Justice, Guidelines for Personal Data Processors 2001:14).

In Finland, the definition of personal data is: "any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household" (cf. Article 3.1).

As long as a person is identifiable this is considered personal data in Finnish law, even though the controller could not identify anybody him or herself. According to the law, the processing of such semi-anonymous data should therefore still comply with the data protection principles. In Finnish practice, however, it is often considered that if actual identification of the data subject requires unreasonable effort and the data de facto is anonymous, it is not necessary to strictly follow the data protection principles (Lehtonen 2004).

Sweden includes the term “indirectly” in its definition of personal data as “all kinds of information that directly or indirectly may refer to a natural person who is alive” (cf. Section 3 of the Swedish DPA). The German FDPA defines personal data as “any information concerning the personal or material circumstances of an identified or identifiable individual” (cf. Section 3 (1)), and the Estonian Personal Data Protection Act adds that personal data is “any data concerning an identified natural person or a natural person to be identified, regardless of the form or format in which such data exists” (Article 4-1).

Norway, Denmark, Spain and Iceland have similar definitions of personal data. In the Norwegian PDA, personal data is defined as "(...) any information and assessments that may be linked to a natural person" (cf. Chapter 1, Section 2.1). According to the Danish Act, personal data entails "(...) any information relating to an identified or identifiable natural person (‘data subject’)" (cf. Chapter 2, 3.1). In the Spanish regulation LOPD, "(...) any information concerning identified or identifiable natural persons" is to be considered personal data (cf. Article 3.a). According to the Icelandic DPA, personal data is defined as: "(...) any data relating to the data subject (identified or identifiable), i.e. information that can be traced directly or indirectly to a specific individual, deceased or living (cf. Article 2.1). According to the legislation of these four countries, no one should be able to identify the data subject if the data is to be considered anonymous.

The UK, however, stands out with regard to the definition of personal data. According to the UK Data Protection Act (DPA), personal data is defined as:

“(…) data which relate to a living individual who can be identified - a) from those data or, b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expressions of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual” (Section 1 (1) of the DPA).

This provision represents a unique position among countries who have implemented the 95/46/EC Directive as it defines data as personal only if the data controller can identify the data subject (Privireal 2005). The provision is controversial as it differs from the definition of personal data provided in the Directive (article 2 (a)), which can be understood as referring to data as personal if *anyone* can identify the data subject directly or indirectly (Beyleveld et al. 2004: 408). Hence, a lot more individual level data falls outside the scope of the privacy regulation in the UK as compared with other EU-countries. One result of this is that the use of personal data in UK-based projects on a European level,may be subject to less restrictions and requirements (e.g. with regard to informed consent) than projects based in other EU-countries.

There is also a variance to be found with regard to whether information regarding deceased individuals is included in the definition of personal data. In Norway, Sweden, Finland, Denmark, the Netherlands, Spain and the UK, one can assume that personal data relates only to living individuals. In Iceland, however, personal data includes any information that can be traced to a specific individual, deceased or living (Article 2.1 in the Icelandic DPA). In Estonia as well, a provision regarding the processing of personal data after death of data subject is included (cf. Article 13 of the Estonian DPA). Thus, both the Estonian and Icelandic data protection regulations represent a break with the other countries included in this comparison.

The various definitions of personal data and anonymity are often an obstacle and a serious barrier for comparative research projects. One example is the problems involved in using administrative data in transnational surveys because of various definitions of anonymity, another is the different consent requirements depending on whether or not the study falls within or outside the scope of law.

5.2.3 Notification requirement

Another obstacle is the different implementations of the Directive's notification duty and the requirement of prior legal approval for the processing of personal data. This makes up a patchwork of various systems across the different EU countries. Each country has its unique system of when different kinds of approvals are necessary, and when simplifications and exemptions from notification duty and prior assessment can be made. For researchers to orientate in this landscape, to coordinate applications and to ensure the timeliness of deadlines across countries, is not an easy task. (For an overview of notification and approval requirements in the countries presented here, see table in Appendix I).

According to the 95/46/EC Directive, Article 18, "Member States shall provide that the controller must notify the supervisory 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". Provided that certain conditions are followed, the notification duty may be simplified or exempted (cf. Article 18).

Further, according to Article 20, "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".

Germany and Sweden, operates either with a general notification duty to the Authority or more likely a continuous control by the appointed data protection officer, for the processing of non-sensitive personal data. In Sweden, there is however an exemption from the notification requirement for non-sensitive personal data if the data subject has consented to the processing (cf. The Swedish Data Inspection Board). The processing of sensitive personal data for research purposes, can however only take place if approved by an ethics committee, due to the Swedish Ethical Review Act. This applies whether or not the subjects of the research have given their consent. In Germany, the processing of sensitive personal data not based on consent must be assessed in advance by the appointed data protection officer (cf. Article 4d of the FDPA).

In Estonia, there is no notification regulation for the processing of non-sensitive personal data. Regarding sensitive personal data however, it is either required to have a legal approval from the Data Protection Inspectorate for the processing, or to have appointed an independent data protection officer. The processing of sensitive personal data not based on consent requires in both cases an ethics approval. Processing of sensitive personal data is registered for a period of up to five years. A processor of personal data is then required to submit a new application for registration (cf. Article 27-3 in the Estonian DPA).

The Finnish Data Protection Act has exempted most research from the notification duty to the Data Protection Ombudsman. It seems, however, that this exemption is applicable only to research that does not utilise sensitive data, and that e.g. registries including sensitive information are to be notified to the Data Protection Ombudsman (Lehtonen 2004). Otherwise, the duty of notification in Finland would concern e.g. the cases where the processing of personal data is outsourced or certain cases where personal data is transferred to countries outside the European Union or the European Economic Area (cf. Article 36, point 2 and 4 of the Finnish PDA). Moreover, the Finnish National Advisory Board on Research Ethics recommends that research establishments arrange ethical reviews for human science with special issues (e.g. intervention in the physical integrity, not based on consent, involving children, security risk etc.).

The Dutch Data Protection Act provides an Exemption Decree with a large number of exemptions and simplifications to the general notification obligation in the DPA. According to Article 16.2 (d) of the Exemption Decree, medical healthcare professionals are exempted from the notification duty when processing personal data about their own patients for scientific or statistical research purposes. In Article 29 of the Decree, the storing of personal data for scientific, statistical or historical research purposes is also exempted from the notification duty.

Article 30 in the decree deals with scientific research and statistics specifically, performed by a scientific research facility. The notification duty does not apply provided e.g. that the research data is de-identified and the directly identifying data is also not kept for more than six months after they have been obtained from the data subject. It is important to keep track of this six-month period and to notify the Data Protection Authority (CBP) or data protection officer of the processing if it is necessary to keep e.g. contact details for longer than six months (de Cock Buning et.al: 2009). However, research projects involving special privacy risks (e.g. not based on consent), must anyhow be approved by the CBP in advance (de Cock Buning et.al: 2009:43).

In Norway, Spain and the UK it is required to notify the processing of both sensitive and non-sensitive personal data. In Spain, notification to the Spanish Data Protection Authority (AEPD) Agencia Española de Protección de Datos)) is required before the processing of personal data is initiated (cf. Article 26.1 of the LOPD). The General Data Protection Register of the AEPD must approve the notification if it complies with the requirements of the LOPD.

According to the Norwegian Personal Data Act, a data controller is obligated to notify the Data Protection Authority in Norway before processing personal data by automatic means or establishing a manual personal data filing system which contains sensitive personal data (cf. Article 31 of the Norwegian PDA). The notification duty applies whether or not the data subjects have given their consent to the processing. When processing non-sensitive personal data, the Data Protection Authority merely establishes an obligation to notify, and a prior approval of the Authority is not required. The processing of sensitive data, however, requires a license from the Authority prior to the processing, whether or not the processing is based on consent (cf. Article 33 of the Norwegian PDA).[11]

[11] On June 5 2008, the new Act on Medical and Health Research was enacted. The Health Research Act applies to medical and health research, which is research on humans, human biological material and personal health information, which aims to generate new knowledge about health and disease. The purpose of the project is decisive; not whether the research is carried out by health professionals or on patients or makes use of personal health information. Research on patient and health information for other purposes, such as social science, is regulated by the Personal Data Act (NSD, Data Protection Official for Research).

In practice the vast majority of research projects (including the processing of sensitive personal data) are exempted from the obligation to notify or to obtain a license from the Data Protection Autority (cf. Section 33:1 of the PDA) provided that the project has been recommended by a Data Protection Official (cf. Section 7-27 of the Norwegian Personal Data Regulation). However, research projects of large scale and long duration, as well as research on large data sets that are not adequately de-identified, are not exempted by this provision. Research projects that lasts for more than 15 years and entails 5000 data subjects or more are considered to be of large scale and of large duration (cf. Note to § 7-27 in the Norwegian Personal Data Regulation).

In the UK under Section 18 and 19 of the DPA, every data controller that processes personal data is obliged to notify the Information Commissioner's Office (ICO), with some exemptions. However, it is sufficient that each university sends a general notification including all the processing of personal data conducted at their institution by researchers and students.

In Denmark, student theses are exempt from the notification requirement. In accordance to changes in the legislation in May 2012, students collecting and processing sensitive personal information based on the explicit consent of the data subjects in connection with their project and thesis writing etc. are exempt from the requirement of notification to the Data Protection Agency under certain conditions. Graduate students are, however, not covered by the exemption. Moreover, non-sensitive data is exempt from the notification requirement in Denmark.

In the new proposal for EU regulation, the obligation to obtain a license is completely revoked for institutions with a data protection officer and is replaced by an obligation for prior consultation by the data protection officer for the processing of personal data that entails specific risk, cf. Article 34 (Kvalheim 2014).

5.3 Exemptions from informed consent for scientific purposes

According to Article 7 of the 95/46/EC Directive, personal data may be processed only if the data subject has unambiguously given his consent or e.g. the processing is necessary for the performance of a task carried out in the public interest.

Further, as stated in the preamble recital (34) of the Directive, Member States are authorised to derogate from the prohibition on processing on sensitive categories of data if important reasons of public interest justifies such processing, such as for instance scientific research. However, it is required to provide specific and suitable safeguards in order to protect the fundamental rights and the privacy of individuals involved.

All the countries presented here, include alternatives to consent-based processing of (sensitive) personal data for research purposes.

The differences involve mostly whether consent is seen as the main condition, and also how strict the conditions for non-consent processing are. Here, it would be interesting to look into the actual practice of the law in each country. However, the cumulative conditions of public interest clearly outweighing the privacy risks of the data subject and that the purpose could not otherwise be achieved, is the main finding in all of the analysed Acts. Even if the provisions regulating exemptions look similar, they are up for highly different interpretations across EU-countries.

The Finnish Personal Data Act sets up these following cumulative conditions for non-consent processing for the "purposes of historical or scientific research", stating that consent is the main condition (cf. Section 14.1):

- the research cannot be carried out without data identifying the person and the consent of the data subjects cannot be obtained owing to the quantity of the data, their age or another comparable reason;
- the use of the personal data file is based on an appropriate research plan and a person or a group of persons responsible for the research have been designated;
- the personal data file is used and data are disclosed therefrom only for purposes of historical or scientific research and the procedure followed is also otherwise such that the data pertaining to a given individual are not disclosed to outsiders; and
- after the personal data is no longer required for the research or for the verification of the results achieved, the personal data file is destroyed or transferred into an archive, or the data in it are altered so that the data subjects can no longer be identified

In the Netherlands, the exemption provision implicates that consent has absolutely priority, unless it appears impossible or would involve a disproportionate effort (Wright and Terstegge 2004). The following cumulative conditions must be met in order to process sensitive personal data for the purpose of scientific research (cf. Article 23-2 of the Dutch DPA):

- 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 express consent and,
- sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent
- it is also lawful to process special (sensitive) personal data if the data has manifestly been made public by the data subject.

Article 44 of the Dutch DPA also states restricted rights of data subjects if personal data is processed by an institution or service for scientific research or statistics. If the necessary arrangements have been made to ensure that the personal data can only be used for statistical or scientific purposes, then e.g. the right to be informed that his or her details are being processed and the right to submit a request to inspect these details do not apply (de Cock Buning et.al: 2009).

Medical professional secrecy is regulated by Book 7 of the Dutch Civil Code. Whereas Article 457 states that disclosure of patients' health information can only take place with the consent of the patient, Article 458.1 provides exemption from consent for the purpose of statistics or scientific research in the field of public health, if:

- seeking consent is not reasonably possible and if, with respect to the performance of the research, such guarantees have been given that the privacy of the patient is not disproportionately prejudiced; or
- seeking consent, taking into account the nature and object of the research, cannot reasonably be required and if the provider of the care has ensured that the information is given in such manner that tracing to individual natural persons is reasonably prevented.

Such disclosure is only possible if:

- the research serves a public interest;
- the research cannot be carried out without the relevant data; and
- to the extent that the patient involved has not explicitly objected to the information being given (Article 458.2 of Book 7 of the Dutch Civil Code) (Burgerlijk Wetboek Boek 7)

The provision indicates that, it is only possible to rely on non-consent alternatives if the nature and object of the research indicates consent cannot reasonably be required. However, the disclosed information still has to be as anonymised or encoded as soon as possible (Wright and Terstegge 2004:282).

The Estonian Personal Data Protection Act states that it is allowed to process personal data without the consent of the data subject for the needs of scientific research with the restriction that data allowing a person to be identified are substituted by a code (cf. Article 16-1). Further, personal identifiable data may be processed for research purposes without consent if the aims of the processing would otherwise not be achievable, there exist a predominant public interest for such processing and the volume of the obligations of the data subject is not changed on the basis of the processed personal data and the rights of the data subject are not excessively damaged in any other manner (cf. Article 16-2).

Otherwise, the Estonian PDA includes a provision regarding deceased, saying that after the death of a data subject, processing of his or her personal data is permitted only with the written consent of e.g. a successor, spouse or relative, if thirty years has not passed from the death of the data subject (cf. Article 13).

In Sweden, sensitive personal data may be processed for research and statistical purposes without the consent of the data subject, if the processing is approved by an ethical review board under the Ethical Review Act. Additionally, provided that the processing is necessary and the interest of society in the project is manifestly greater than the risk of improper violation of the personal integrity of the data subject (cf. Section 19 of the Swedish DPA). If the processing has been approved by an ethical committee these conditions are considered to be met.

In the Danish Act, sensitive private personal data may be processed for the sole purpose of carrying out statistical or scientific studies of significant social importance and where such processing is necessary in order to carry out these studies (cf. Section 10.1).

The Danish Act thus provides an opportunity for the processing of personal data for research purposes without the prior consent of the data subject. Hartlev (2004) consequently states that, in relation to research data, the subject's powers to control the use of personal data are limited. Furthermore, the use of personal data for research purposes may not be obvious to the data subject as they are not always informed about the possible use of data. If the demand for data appears after the collection, data may be passed on to other researchers (third parties) without the knowledge of the data subjects. The third party's duty to inform the data subject may be exempted in this situation, and furthermore, the data subject's right to access may also be set aside according to the Act on Processing of Personal Data. At first glance, this legal situation is not ideal from a data protection point of view. Hartlev, however, remarks that one must consider the legal safeguards provided by the Act in connection with the use of data for research purposes. These safeguards protect the data subject's privacy towards the general public as results from the research project may only be published in an anonymous form. Furthermore, the data may not be used for other purposes than research and may not be handed over to third parties (other researchers) without the prior authorisation of the Supervisory Authority (cf. Section 10.2 and 10.3). It is also important to notice that the Act on Processing of Personal Data should be seen in context with other rules and regulations in the research field. The Act of a Scientific Ethical Committee System will, for instance, require the consent of the data subject when he or she is directly involved as a research subject.

In Spain, the processing of personal data may be exempted from obtaining the consent of the data subject if for instance the transfer of the data is made between public administrations and "concerns the retrospective processing of the data for historical, statistical or scientific purposes" (cf. Article 11.2 e of the LOPD).

The Norwegian Personal Data Act allows for the processing of sensitive personal data without consent if the processing is necessary for historical, statistical or scientific purposes, and the public interest clearly exceeds the possible disadvantages for the data subjects (cf. Article 9 h). However, in order to allow processing based on this provision, the researcher must in addition establish that it is impossible to obtain consent without seriously damaging the research. Otherwise this approach will be seen as violating the respondent's privacy interests.

The degree of disadvantage for the data subject is linked to the extent to which the proposed use of data is considered to differentiate from the original use of data. Regardless of these considerations, the Norwegian Data Protection Authority tends to be very reluctant to use the exemption for research. The conditions of necessity and public interest are applied strictly, and overall non-consent alternatives are rarely accepted, as long as obtaining consent is feasible (Kvalheim 2004).

When research projects are exempted from consent, e.g. in register based research, it is nonetheless considered whether it is possible to give individual information about the processing to the data subjects, with the offering of a withdrawal possibility. This is seen as an argument to lower the disadvantages the non-consent based processing entail.

In some countries, e.g. the Netherlands and Germany, it is explicitly stated that it is lawful to process sensitive personal data if it has already been made public by the data subject. However, legislation applying to for instance social media research tends to be very different across Europe, making place for many obstacles within cross country research in this field.

For example, the limits of what could be considered as data which has been made public have been up for debate in a Norwegian context, regarding social media research. In 2009, a Norwegian social media site closed down because all its members moved over to Facebook instead. For historical and research purposes, it was applied for further storing of the personal information available for all of the community's members. The Data Protection Authority however argued that this online community consisting of 750 000 members, should be considered as a private arena, when shared information was visible only for members. The storing therefore should be based on consent, they argued. This decision was however appealed to the Privacy Advisory Board, whereas the final conclusion (some years later) was that an online community consisting of this large number of members is not to be understood as private in a common understanding of the word "private", also referring to the factor that whoever could join the community, without any restrictions. The information could then at last be stored for research purposes without collecting consents (PVN 2012-03).

Similarly in Iceland, the processing of personal data may be exempted from consent if e.g. the processing is necessary for a task that is carried out in the public interest (cf. Article 8.5 in the Icelandic DPA). The Icelandic Data Protection Authority can moreover authorise the use of alternatives to consent if the processing of data is apparently in the vital interests of the public or individuals, including the interests of the data subject. The processing of sensitive personal data is prohibited unless one of the conditions in Article 8.1 in DPA, and one or more of the requirements in Article 9 of the DPA has been fulfilled. For instance, a condition stated in Article 9.9 in the DPA is that the processing is necessary for the purposes of statistical or scientific research, provided that the privacy of individuals is protected by means of specific and adequate safeguards.

Overall, consent is considered the main condition for the processing of personal data in data protection legislation in the countries presented here. However, the UK and Germany represent somewhat special cases in this regard.

Among the conditions for processing personal data listed in the DPA of the UK, consent (cf. Schedule 2 or explicit consent cf. Schedule 3) is simply one of the alternatives. For this reason, Beyleveld et al. claims that there is nothing in the UK DPA that explicitly states consent of the data subject as a necessary condition for legitimate processing of sensitive data (2004: 417). However, as all UK legislation should (if possible) be interpreted and be compatible with the provisions of the European Convention on Human Rights (ECHR), Beyleveld et al. assert that:

(…) it is arguably that consent must be obtained for the processing of sensitive personal data *unless* conditions that would satisfy a breach of Article 8 (1) of the ECHR are satisfied [i.e. Right to respect for private and family life] (ibid.).

In Germany, the law does not distinguish between the different alternatives for lawful processing of personal data, whether they require consent or not. Consequently, it should be sufficient to use alternatives to consent as long as the processing is in accordance with a specific provision (Kühn 2004). According to the FDPA, collection of special categories of personal data within research is lawful if the following cumulative conditions are met (Section 13.2 no. 8):

- it must be necessary for the purposes of scientific research
- the scientific interest in the research must significantly outweigh the interests of the data subject to rule out the possibility of processing and
- the purpose of the research could not be achieved in any other way or would require a disproportionate effort

It is also lawful to process special categories of personal data if it has already been made public by the data subject.

In the proposal for the General Data Protection Regulation, the exemptions from consent for the use and storage of personal data have become significantly narrower (Kvalheim 2014). It is however specifically mentioned that the processing of special categories of personal data shall not be prohibited if processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83 (cf. Article 9.2 (i)). Whereas Article 83 of the proposal includes the following conditions:

- the purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;
- data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects.

These requirements could mean that research would almost always require consent as the legal basis for processing of personal data. The need for specific consent is a particular problem in this regard (Kvalheim 2014).

5.4 Preservation

According to the 95/46/EC Directive, Article 6 (b), "further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards".

It seems that all of the Data Protection Acts in our sample allow preservation of (sensitive) personal data for research purposes, with quite similar conditions. The German Federal Data Protection Act does not mention further storage for research purposes in particular, but the Act includes preservation for further processing/use in the term "recording" (cf. Section 3.4.1). Thus, the conditions for preservation for other purposes than the controller is responsible for and for which the data were collected, are:

- if based on consent or if necessary for the purposes of scientific research, where the public interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection and;

- the purpose of the research cannot be achieved in any other way or would require a disproportionate effort (cf. Section 14.5 of the FDPA).

The Estonian Personal Data Protection Act, states that collected personal data may be processed for the purposes of scientific research regardless of the purpose for which the personal data was initially collected. Personal data collected for scientific research or official statistics may be stored in a coded form for the purposes of using it later for scientific research or official statistics (cf. Article 16-4).

According to Section 35 of the Finnish PDA, a personal data file which is significant for purposes of scientific research or otherwise may be transferred for archiving to an institution of higher education or to a research institute or authority operating on a statutory basis. It is, however, required that the National Archives have granted permission for such archiving. The National Archives may grant corporations, foundations and institutions a permission to archive personal data files compiled in their own activities and fulfilling the requirements above. In the permission, the National Archives shall lay down rules for the protection of the files and for the monitoring of the use of personal data. Before granting such permission, the National Archives shall reserve the Data Protection Authority an opportunity to issue an opinion on the matter.

The Swedish Personal Data Act states that the processing of personal data for historical, statistic or scientific purposes shall not be regarded as incompatible with the purposes for which the information was collected. And further, that personal data may be kept for historical, statistic or scientific purposes for a longer time than necessary for the original purpose. However, personal data may not in such cases be kept for a longer period than is necessary for these purposes (cf. Section 9 of the Swedish PDA).

The Dutch DPA also allows that personal data may be kept longer for historical, statistical or scientific purposes, if the data controller has made the necessary arrangements to ensure that the data concerned are used solely for these specific purposes (cf. Article 10.2). It does not matter in this case whether the data was originally collected for the said historical, scientific or statistical purpose, as long as safeguards are taken to ensure that the data are stored (and

reused) exclusively for research purposes (Ministry of Justice, Guidelines for Personal Data Processors 2001:40).

In Spain, personal data subjected to processing may not be used for purposes incompatible with those for which they were originally collected. However, the further processing of the data for historical, statistical or scientific purposes shall not be considered incompatible purposes (cf. Article 4.2 in the LOPD).

Similarly in Denmark, personal data must be collected for specified, explicit and legitimate purposes and further processing must not be incompatible with these purposes. Further processing of data which takes place exclusively for historical, statistical or scientific purposes shall not be considered incompatible with the purposes for which the data were collected (cf. Chapter 4 Article 5.2 in the Danish Act).

Also in Iceland, the further processing of personal data for historical, statistical or scientific purposes shall not be considered incompatible to the specified, explicit, apposite purposes for which the personal data originally was obtained provided that proper safeguards are adhered to (cf. Chapter 2: Article 7.2 of the Icelandic DPA).

In the UK, personal data shall not be kept for longer than is necessary for the original purpose or purposes, according to the fifth data protection principle (cf. Schedule 1, part 1 (5) of the UK DPA). However, this principle does not apply to personal data processed only for research purposes (Bristol 2014a). Research activity is exempt from this requirement provided that it has met all the conditions for exemption for research, history and statistics purposes (cf. Section 33 of the UK DPA).

Moreover, the ICO asserts that there are often good grounds for keeping personal data for historical, statistical or research purposes. In their Guide to Data Protection, the ICO states:

> "The Data Protection Act provides that personal data held for these purposes [i.e. historical, statistical or research purposes] may be kept indefinitely as long as it is not used in connection with decisions affecting particular individuals, or in a way that is likely to cause damage or distress. This does not mean that the information may be kept forever – it should be deleted when it is no longer needed for historical, statistical or research purposes" (ICO).

The Norwegian Personal Data Act allows preservation of personal data for historical, statistical and scientific purposes, on the conditions that the public interests clearly extend the disadvantages for the data subjects (cf. Article 11 and 28). The main rule in this regard is that long-term storage of personal data should be based on consent, in addition to appropriate safeguards.

The conditions for the processing and treatment of personal information are laid out in Norwegian Personal Data Act Article 8 and Article 9, where it is stated that personal information can only be processed if the data subject has consented or the access to such treatment is provided by law (or if the treatment / processing is necessitated by a set of specified criteria, see Article 8, letter a-f and Article 9, letters a-h).

The Norwegian Data Protection Authority, in their guidance, emphasise that they find it legislative and ethically problematic to allow processing for new and incompatible research purposes, if the data were originally collected based on the consent of the data subject. This is seen as a breach of the contract (Kvalheim 2004). In addition to the above mentioned safeguards, the Personal Data Act requires notification every third year of the processing (including storing) of personal data, as well as the licensing requirements from the Authority prior to processing. The license will normally include requirements with regard to future archiving of personal data.

In the proposed General Data Protection Regulation, a basis for the processing of sensitive personal data by archive services has been added, in which storage for research purposes is specifically mentioned: the processing of special categories of personal data shall not be prohibited if processing is necessary for archive services subject to the conditions and safeguards referred to in Article 83a (cf. Article 9 (ia)). Whereas Article 83a formulates that once the initial processing for which they were collected has been completed, personal data may be processed by archive services for historical, statistical or scientific research purposes, in accordance with the rules set out in the Regulation, specifically with regard to consent and the right to object.

The amount and diversity of research data in the SSH has been increasing steadily. Researchers study language data from, e.g., social media, websites, and audio-visual contents from the media, and generate new datasets by means of annotation, aggregation, etc. New types of research data pose several challenges for their long-term preservation and reuse.

Long-term preservation can be defined in a broad sense as a process that encompasses "policies, strategies and actions that ensure permanent access to digital content over time" (DASISH 2014a). Data preservation may include transferring data, e.g., from a researcher to a repository;[12] the data storage and access management in that repository; and the process of sharing and (re-)using data stored in the repository (DASISH 2014a).

Aspects of trust and certification play an important role in this process. Data depositors want to be sure that their data is discoverable and accessible on clearly specified conditions and with an agreed service level for a long time. Data transferred in the care of a repository for the purpose of preservation and reuse must be accompanied by clear agreements specifying the responsibilities of the depositor and repository, clearing any legal issues regarding access to the data, such as copyright, and specifying legal and ethical guidelines which end users must adhere to.

A potential conflict of interest can arise between the advancement of society in general and scientific progress. "The types of data that have the potential to harm and infringe on the research subjects' personal rights may be in conflict with the possible utility and use of data, are often a vital resource for academic research across a wide range of disciplines" (DASISH 2014a). A related concern for research ethics is "the risk of treating research subjects as mere means to an end by disregarding data protection and privacy issues" (DASISH 2014a).

Trust and certification

For a repository to become certified and trusted, several procedures exist, based on audits and self-assessment. In one approach, checklists for specific criteria are produced, in which repositories are required to be able to fulfil and document in order to obtain certification. An example of the checklist approach is the Trustworthy Repositories Audit and Certification (TRAC).[13] TRAC specifies a set of criteria and a checklist that allow digital repositories to assess their capability to reliably store, migrate, and provide access to digital content.

Alternatively, toolkits are developed that seek to guide a repository through a risk assessment procedure that enables the repository to evaluate, through self-assessment, its ability to fulfill

[12] We use the term *repository* for a research data archive, research infrastructure or similar data deposit service.
[13] http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

its self-specified goals. Some of the most prominent frameworks for the second approach include Digital Repository Audit Method Based On Risk Assessment (DRAMBORA),[14] Data Seal of Approval (DSA),[15] DIN 31644,[16] and ISO 16363.[17] DRAMBORA presents a methodology and a toolkit that focuses on identification, evaluation and management of likelihood and potential impact of risks on the repository.

DSA is a set of 16 guidelines that data repositories or archives must demonstrably comply with. The DSA guidelines include the description and documentation of work processes such as handling software, hardware and data migration. In order to qualify for a DSA, an archive must meet e.g. the requirement that the research data is reliable and available in a usable format. DIN 31644 is a set of criteria that define 34 standardised requirements for the setup and management of digital archives. ISO 16363 certification is a recommendation to be used as the basis for providing audit and certification of the trustworthiness of digital repositories. It provides a detailed specification of criteria by which digital repositories can be audited.

Although complying with one of these standards or acquiring a certificate is a good thing, it does not necessarily "create an understanding for the researcher about the processes and responsibilities involved in storing and preserving data, nor does it address concerns which might be specific to a certain community or researcher. The careful design and communication of policies and licensing with respect to these concerns and requirements is therefore of utmost importance" (DASISH 2014b).

5.5 Access and reuse

Policies for access and (re-)use to the data resources in a repository must be agreed on by the data provider and the repository. These policies generally take the form of general terms of service for the whole repository, supplemented by specific deposit agreements for each data resource. These policies together define the legal and contractual framework that regulates, among other things, issues related to copyright and ethics. They also define the responsibility of the stakeholders with respect to the transfer, preservation, access and (re-)use of the data,

[14] http://www.repositoryaudit.eu/
[15] http://www.datasealofapproval.org/
[16] http://www.nabd.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738855&artid=147058907
[17] http://www.iso16363.org/

including liability for loss or damage of deposited materials. The policies also address "the requirements in terms of licensing and copyright clarification" (DASISH 2014c).

Accordingly, data providers are usually encouraged or required to attach a license to their data which defines access and re-use restrictions of these data. Repositories often rely on the widely used standard license schemes, such as Creative Commons,[18] Open Data Commons,[19] and GNU General Public License.[20] Alternatively, repositories, projects or sectors have prepared their own license agreements, such as those prepared by META-SHARE,[21] CLARIN,[22] CESSDA[23] and DANS.[24] Finally, users may be allowed to specify customised terms of use (so-called 'bespoke' licenses).

One of the central questions to be addressed by the archive's policies and licenses is to what extent the access to data will be open, restricted or controlled. In open access, the data are free for all to read and copy, but there may be conditions such as attribution of the data to its producer. In restricted access, confidential or sensitive information needs to be secured. In a controlled access, access rights might depend on user identity and location.

Restricting and/or controlling access may be motivated by the need to protect, e.g., data involving human subjects, copyrighted, sensitive or confidential data, to be used for research and educational purposes. Accordingly, the archive may require users to be authenticated before being authorised, in order to ensure that only users with the appropriate credentials get access to these specific data. In addition, the use of such data may be restricted to specific purposes. Users may be required to sign a Terms of Service (TOS) agreement[25] and one or more End User License agreements (EULA).[26] An EULA "is an agreement between the repository and the end users of a deposited resource. It regulates the conditions under which the users can access and exploit the resource" (DASISH 2014a). In such an agreement, the user agrees on certain conditions, "e.g. not to use data for commercial purposes or identify any potentially identifiable individuals" (DASISH 2014d). "Terms of use which are not

[18] http://creativecommons.org/
[19] http://opendatacommons.org/
[20] http://www.gnu.org/licenses/licenses.html#GPL
[21] http://www.meta-net.eu/meta-share/licenses
[22] https://kitwiki.csc.fi/twiki/bin/view/FinCLARIN/ClarinEULA
[23] http://www.cessda.org/sharing/dissemination/1/
[24] http://www.dans.knaw.nl/en/content/dans-licence-agreement-deposited-data
[25] For an example of Terms of Service (TOS) agreement, see https://kitwiki.csc.fi/twiki/pub/FinCLARIN/FinClarinLegal/CLARIN-TOS-v0.95.rtf.
[26] An example of an end user agreement for CLARIN is available under the following link https://kitwiki.csc.fi/twiki/bin/view/FinCLARIN/ClarinEULA.

specific to a particular resource, but which apply for all repository services, are brought together in the terms of service agreement" (DASISH 2014a).

In case some of the resources are subject to additional ethical restrictions, the user may also be required to sign a Data User Agreement.[27] Further access regulations for confidential data may include "placing confidential data under embargo for a given period of time until confidentiality is no longer pertinent; providing access to approved researchers only; providing secure access to data through enabling remote analysis of confidential data but excluding the ability to download data" (DASISH, 2014d).

In sum, access to the resources distributed by a repository or archive may be restricted depending on various parameters, including the license type, the user identity, and the type of data.

In the 95/46 Directive, it is explicitly specified that 'further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards', cf. Article 6 (b).

The different Personal Data Acts presented here thus allow for the reuse of personal data for research purposes based on certain safeguards, for data originally created for a different purpose.

Article 9.3 of the Dutch DPA provides that the further processing of personal data for historical, statistical or scientific purposes shall not be regarded as incompatible as long as the data controller has made the necessary arrangements to ensure that the further processing is carried out solely for these specific purposes.

This means that the reuse of files for scientific research that has already been created is permitted, even if the file was created for a different purpose (de Cock Buning et.al: 2009:43). Regarding the reuse of sensitive data or data that is subject to professional confidentiality, the main rule is anyhow that the reuse shall be based on consent or meet the conditions for exemption from consent.

The Finnish PDA also states that later processing of personal data for purposes of historical, scientific or statistical research is not deemed incompatible with the original purposes (cf.

[27] For example of a Data User agreement, see the agreement provided by the CLARIN Center at the Saarland University at https://fedora.clarin-d.uni-saarland.de/ressources/DataUserAgreement.en.pdf.

Section 7). So, if sensitive data is of scientific value or is historically unique, a request for permission to archive data can be submitted to the National Archives (The National Advisory Board on research ethics' proposals). Secondary users of data should be requested to sign an agreement on the conditions set for secondary research and if needed also a pledge of confidentiality (TENK: Ethical principles of research in the humanities and social and behavioural sciences and proposals for ethical review). One of the general conditions of processing personal data is that the data controller must ensure that the data subject can have information on the data controller, on the purpose of the processing of the personal data, on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question. The PDA, however, states that there is no right of access for data subjects to the data on him/her in a personal data file, if the data in the file are used solely for historical or scientific research or statistical purposes (cf. Section 27.1.3).

In Spain, personal data shall be erased when they have ceased to be necessary or relevant for the purpose for which they were obtained or recorded (cf. article 4.5 of the LOPD). Moreover, personal data shall not be kept in a form which permits identification of the data subject for longer than necessary for the purposes for which they were obtained or recorded. On a regular basis, the procedure shall be determined by which, exceptionally, it is decided to keep the entire set of particular data, in accordance with the specific legislation, because of their historical, statistical or scientific value.

According to the second data protection principle of the UK DPA (cf. Schedule 1, part 1 (2)), personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes. However, the second part of this principle does not apply to the further processing of personal data made only for research purposes (University of Bristol 2014a). Research activity is exempt from this requirement provided that it has met all the conditions for exemption for research, history and statistics purposes (cf. Section 33 of the DPA).

In Norway, there are two main conditions for access and reuse of personal data. Either the processing should be based on the informed consent of the data subject, or it should be exempted from the duty of confidentiality. The reuse of personal data for a different purpose than the original one must be assessed according to the provisions of §§ 8 and 9 in the Norwegian Data Protection Act. If the data that is sought reused originally was collected on

the basis of consent (cf. §§ 8a, 9a), the reuse of data is restricted according to what the participants have consented to and been informed about.

According to the Norwegian Data Protection Authority it is disloyal to the participants if the researcher disregards the "agreement" they made with the participants, and decide to use the data for other purposes than what was agreed in the first place (Norwegian Data Protection Authority 2005). The Data Protection Authority therefore often requires that new consents are collected in case of the reuse of data for new purposes.

In Denmark, the requirement to inform the data subject shall not apply where data are processed solely for scientific purposes or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics (cf. Chapter 9 article 32: 4 of the Danish Act).

Similarly in Iceland, the data subject's right of access under Article 18 does not apply to data which are used solely for statistical processing or scientific research, provided that their processing cannot have direct influence on the interest of the data subject (cf. article 19 of the Icelandic DPA).

In the new EC proposal, the provision specifying that research shall not be considered as incompatible has been removed from the regulation altogether. Seen in conjunction with other proposed amendments in draft regulation, particularly with those that tighten requirements for consent for the processing of health data and sensitive data, the balance in the legislation is clearly shifted in favour of data protection at the expense of research opportunities (Kvalheim 2014).

5.5.1 Copyright

"Copyright is a legal notion that gives exclusive rights to the holder (who need not necessarily be an individual) copyrighted work, i.e. the result of intellectual creativity" (DASISH 2014e). Digital materials are easily copied and re-distributed, but such activities may infringe on IPR unless the necessary exceptions exist, or specific permissions have been obtained from rights

holders. Infringements of copyright can refer to "[a]ny use of copyrighted material by others that is not licensed or authorised, even if it is for educational or research purposes" (DASISH 2014f).

Copyright holders can determine which access, reuse or distribution is permitted, and if these operations are subject to fees. They are particularly concerned with potential infringements of copyright and controlling access (Digital Preservation Coalition 2008). They may take legal action against such infringements (i.e. pursue infringements and enforce copyright through various ways). Likewise, "repositories may pursue actions against copyright infringements and violations of conditions of use, such as cancelling the access to the resource" (Digital Preservation Coalition 2008).

Current IPR legislations in Europe are quite complex and vary from one country to another.[28] For instance, in 2014 the UK adopted a law defining 'fair dealing' which allows copying for research and some other purposes. In Norway, researchers can apply to the government for an exception from copyright. Some other countries have no such exceptions. Depending on the country-specific legislations and the work agreements between researchers and their employers, it may be the creators of research data or their organisations who hold the rights to the data which has been produced. Such differences are obstacles for cross-border cooperative research.

In most cases, therefore, access to data that requires copying and must be made public to others requires explicit arrangements with the copyright holders. A convenient way of managing the IPR of data is through licensing without transferring ownership. To that end, researchers or repositories sign depositors' license agreements which specify rights and restrictions to the use of data. In particular, such agreements suggest an End User Licence Agreement (EULA) based on Creative Commons or other licenses mentioned above.

In sum, it is essential for any work on research data, as well as for repositories holding and managing research data, to address the clearance of copyright and any other IPR at an early stage. If the legal ownership and rights are unclear, it may be legally impossible for any users to get access to the data or to disseminate the data to others.

[28] See chapter 3 for a detailed discussion of issues with respect to IPR legislations in Europe.

6. Conclusion

This handbook has been intended as a concise introduction to some complex legal and ethical issues that researchers in the Social Sciences and Humanities ought to be aware of when using private or copyrighted data.

With respect to copyrighted information, the diversity in law and legal practice across Europe is a barrier for cooperative research and data sharing across borders. As long as there are no Europe-wide exemptions for copying and distributing research data which contains copyrighted information, researchers are therefore advised to check who owns the rights to the data and under which conditions it may be handled and distributed. Unless the data is entirely in the public domain, it may be necessary for researchers to make and observe license agreements with the right holders.

Three main issues have been presented in this handbook regarding the regulation of personal (or private) data: First, there are various definitions of personal data. At one end of the scale, UK's legislation refers to data as personal only if the *data controller* can identify the data subject. At the other end of the scale, in countries like Estonia and Norway, any data concerning an identified person is defined as personal data, regardless of the form or format in which such data exists. In between the two endpoints of the scale, e.g. Germany and the Netherlands allow for a more flexible interpretation of what is defined as personal data. For instance, the Dutch Act leaves it open as to who can identify the data subject. Consequently, the various definitions of personal data which determine whether the processing of data falls within the scope of the privacy regulation or not, have significant impact on conditions under which research operates in the various countries. These variations regarding what is considered anonymous data affect the demands for obtaining consents and the possibilities for preservation as well as reuse of the data. As a result, the quality of research data that researchers can access without data protection regulations varies, which in turn gives richer data available for analysis in some countries compared to others. This situation represents a severe obstacle for comparative cross country research in particular.

Second, the patchwork of approval requirements and bodies across Europe constitute another barrier for research. In some countries, such as the UK, a general notification to the Data Protection Authority is sufficient, whereas in other countries (e.g. Norway and Sweden), it is required to obtain legal approval regardless of whether the processing is based on consent or

not. Due to these variations, it is suggested in the proposal for a new EU data protection regulation that obtaining approvals from the Authority should be replaced by a duty to register the processing and in cases involving specific risks, to conduct a prior consultation of a data protection officer.

Though there still is some uncertainty connected to when the proposed GDPR will become law and it is unclear at this point what the final regulation would look like, the intension is to reduce the fragmentation of data protection regimes, including both laws and supervisory systems across Europe. The concern from the research point of view is that the legal framework conditions within the SSH research domain might be limited. There is a clear tendency in the proposal towards strengthening the right to personal privacy and control of own personal data at the expense of researchers access to personal data.

7. References

- 95/46/EC Directive. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [Internet]. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. [Accessed 05 December 2014].

- Allebeck, Peter. 2002. "The revised Helsinki declaration: Good for patients? Good for public health?". *Scandinavian Journal of Public Health*, vol. 30: 1. Pp. 1-4.

- Baker, S., Beyleveld, D., Wallace, S., and Wright, J. 2005. "Research Committees and the Law in the UK", in Research Ethics Committees, Data Protection and Medical Research in European Countries, D. Beyleveld, D. Townend and J. Wright (eds.). Aldershot: Ashgate. pp. 271-289.

- Beyleveld, D., Grubb, A. Townend, D., Morgan, R. and Wrigh, J. 2004. "The UK's Implementation of Directive 95/46/EC", Beyleveld, D, Townend, D., Rouille-Mirza, S. and Wright, J. (eds.). *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*. Aldershot: Ashgate, pp. 403-428.

- Danish Act on Processing of Personal Data, 2000. The Act on Processing of Personal Data No. 429 of 31 May 2000 [pdf] Available at: <http://www.coe.int/t/dghl/standardsetting/dataprotection/national%20laws/DANEMARKThe%20AAc%20on%20Processing%20of%20Personal%20Data.pdf>. [Accessed 25. February 2014].

- Danish Act on Research Ethics Review of Health Research Projects, 2011. DNVK [online] Available at: <http://dnvk.dk/English/actonabiomedicalresearch.aspx>. [Accessed 25. February 2014].

- Danish Data Protection Agency [online]. Available at: <http://www.datatilsynet.dk/english/>. [Accessed 25. February 2014].

- Danish Data Protection Agency. *Studerendes specialoppgaver mv, 2012*. [online] Available at: <http://www.datatilsynet.dk/erhverv/studerendes-specialeopgaver-mv/>. [Accessed 25. February 2014].

- de Cock Buning M, Ringnalda A. and van der Linden T, 2009. *The legal status of raw data: a guide for research practice* [pdf]. Available at: <http://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2009/SURFdirect_De+juridische+status+van+ruwe+data_wegwijzer_ENG.pdf> [Accessed 18 August 2014].

- Draft EU data protection regulation adopted by the European Parliament, 12 March 2014. Available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+20140312+SIT-01+DOC+WORD+V0//EN&language=EN>. [Accessed 8 December 2014].

- Dutch Data Protection Authority (CBP): *Notification and preliminary examination* [online]. Available at: <http://www.dutchdpa.nl/Pages/en_ind_cbp_taken_melden.aspx> [Accessed 7 June 2014].

- Dutch Exemption Decree, 2001 [online]. Available at: <http://wetten.overheid.nl/BWBR0012461>. [Accessed 8 December 2014].

- Dutch Ministry of Justice, 2001. *Guidelines for Personal Data Processors (Personal Data Protection Act)* [pdf]. Available at: <http://www.privacy.nl/uploads/guide_for_controller_ministry_justice.pdf>. [Accessed 7 June 2014].

- EC (2014). Report on the responses to the Public Consultation on the Review of the EU Copyright Rules. Available at: http://ec.europa.eu/internal_market/consultations/2013/copyright-rules/docs/contributions/consultation-report_en.pdf. [Accessed 12 November 2014].

- EC Press Council Press Conference, 2014. "Today's Justice Council: A Council of Progress: Justice Council Press Conference", Luxembourg 6 June 2014. Available at: < http://europa.eu/rapid/press-release_SPEECH-14-431_en.htm> [Accessed 18 December 2014].

- Estonian Personal Data Protection Act, 2008 [online]. Available at: <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete+kaitse>. [Accessed 4 June 2014].

- European Commission [online]. Available at: <http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm>. [Accessed 5 December 2014].

- European Commision, Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012. [online] . Available at: <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>. [Accessed 17 Dec. 2014]

- Finnish Advisory Board on Research Ethics, 2009. *Ethical principles of research in the humanities and social and behavioural sciences and proposals for ethical review* [pdf]. Available at: <http://www.tenk.fi/sites/tenk.fi/files/ethicalprinciples.pdf> [Accessed 9 September 2014].

- Finnish Advisory Board on Research Integrity: *Ethical review in human sciences* [online]. Available at: <http://www.tenk.fi/en> [Accessed 9 September 2014].

- Finnish Personal Data Act, 1999 [pdf] Available at: <http://www.finlex.fi/fi/laki/kaannokset/1999/en19990523.pdf> [Accessed 10 September 2014].

- German Federal Commissioner for Data Protection and Freedom of Information [online]. Available at: <http://www.bfdi.bund.de/EN/Home/homepage_node.html>. [Accessed 18 June 2014].

- German Federal Personal Data Protection Act, 2009 [online]. Available at: <http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile>. [Accessed 18 June 2014].

- Hartlev, M.,2004. The Implementation of Data Protection Directive 95/46/EC in Denmark. In: D. Beyleveld et.al. Ed. 2004. *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*. Ashgate.

- Health Research Authority, 2013. Summary of the role, structure and functionality of Research Ethics Committees within the Health Research Authority in England [Internet]. Health Research Authority. Available at: http://www.hra.nhs.uk/documents/2013/10/national-research-ethics-service-summary-ver-1.pdf, [Accessed 05 December 2014].

- Icelandic Data Protection Act (DPA). (2000) Act on the Protection of Privacy as regards the Processing of Personal Data, No. 77/2000 of May 10, 2000 [Internet]. Available at: <http://www.personuvernd.is/information-in-english/greinar/nr/438>. [Accessed 15 January 2014].

- ICO. The Guide to Data Protection [Internet]. Information Commissioner's Office (ICO). Available at: http://ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf, [Accessed June 19 2014].

- Imperial College London, 2014. Ethics approval for health-related research [Internet]. Imperial College London, available at: http://www3.imperial.ac.uk/clinicalresearchgovernanceoffice/projectplanning/ethicsapproval/ethicsapprovalforhealthrelatedresearch, [Accessed June 19 2014].

- Intellectual Property Office (UK), 2014. Government takes important step towards modernising copyright (official press release). Available at: https://www.gov.uk/government/news/government-takes-important-step-towards-modernising-copyright. [Accessed 23 June 2014].

- Kulturdepartementet (Norway). Lov om opphavsrett til åndsverk m.v. (Åndsverksloven.) [the Norwegian Copyright Act]. Available at: http://lovdata.no/dokument/NL/lov/1961-05-12-2. [Accessed 23 June 2014].

- Kvalheim, V, 2004. Implementation of the Data Protection Directive in Relation to Medical Research in Norway. In: D. Beyleveld, D. Townend, S. Rouille-Mirza and J. Wright, ed. 2004. *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*. Ashgate. pp. 289-305.

- Kvalheim, V, 2014. EU-parlamentet har vedtatt forslag om ny personvernlovgivning: Styrker personvernet – innsnevrer mulighetene for forskning, Personvernombudet for forskning, NSD, 27.03.2014 [online] Available at:<http://www.nsd.uib.no/personvern/om/eu.htmlZ [Accessed 03 April 2014].

- Kvalheim, V, 2014. *EU Parliament vote on new Data Protection Legislation* [pdf]. Available at: <http://www.cessda.net/news/EU-PrivacyRegulationNegotiatingMandate_Implications.pdf>. [Accessed 5 December 2014].

- Kühn, H. 2004. The implementation of the Data Protection Directive 95/46/EC in Germany. In: D. Beyleveld, D. Townend, S. Rouille-Mirza and J. Wright, ed. 2004. Implementation of the Data Protection Directive in Relation to Medical Research in Europe. Ashgate. pp. 121-140.

- Lehtonen. L.2004. The Implementation of EU Directive 95/46/EC and the Protection of Sensitive Health Data in Medical Research in Finland. In: D. Beyleveld, D. Townend, S. Rouille-Mirza and J. Wright, ed. 2004. Implementation of the Data Protection Directive in Relation to Medical Research in Europe. Ashgate. pp. 87-95.

- LIBE draft report 2012/0011 (COD), 2012 [pdf]. Available at: <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf>. [Accessed 5 December 2014].

- LOPD. Organic Law 15/1999 of 13 December on the Protection of Personal Data (LOPD). Agencia Española de Protección de Datos (AEPD). [Online]. Unofficial English translation. Available at: http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/Ley_Orgaica_15-99_ingles.pdf. [accessed 17.07.2014].

- Norwegian Data Protection Authority [online]. Available at: <http:// www.datatilsynet.no>. [Accessed 24. February 2014].

- Norwegian Data Protection Regulation. Regulations on the processing of personal data (Personal Data Regulations, 200. Available at: < http://www.datatilsynet.no/English/Regulations/Personal-Data-Act1/>. [Accessed 05 December 2014].

- Norwegian Personal Data Act. Act of 14 April 2000 No. 31 relating to the processing of personal data. Available at: < http://www.datatilsynet.no/Global/english/Personal_Data_Act_20120420.pdf>. [Accessed 5 December 2014].

- NSD, Data Protection Official for Research. Frequently asked questions. Available at: < http://www.nsd.uib.no/personvern/en/notification_duty/faq.html?id=5>. [Accessed 20 February 2015].

- OECD, 2007. OECD Principles and Guidelines for Access to Research Data from Public Funding. Available at: http://www.oecd.org/science/sci-tech/38500813.pdf. [Accessed 23 June 2014].

- Privireal, 2005. UK- Data Protection [Internet], Privireal: privacy in Research Ethics and Law. Available at: http://www.privireal.org/content/dp/uk.php, [accessed on June 19 2014.]

- Privireal, 2005. "Spain: RECs and medical research". Privireal: Privacy in Research Ethics and Law. [Online]. Available at: http://www.privireal.org/content/rec/spain.php, [accessed 17.07.2014].

- PVN-2012-03. «Nettby. Personvernnemndas avgjørelse av 23. oktober 2012» [online] Available at: <http://www.personvernnemnda.no/vedtak/2012_03.htm>. [Accessed 12. March 2014].

- Romeo-Casabona, Carlos Maria and Nicolas, Pilar, 2005. "Research Ethics Committees in Spain", in *Research Ethics Committees, Data protection and medical Research in European Countries*, D. Beyleveld, D. Townend and J. Wright (eds.). Aldershot, Burlington: Ashgate. Pp. 233-244.

- Swedish Data Inspection Board [online]. Available at: <http://www.datainspektionen.se/in-english/>. [Accessed 25. February 2014].

- Swedish Ethical Review Act, 2003. *The Act concerning the Ethical Review of Research Involving Humans* [pdf] Available at: <http://www.epn.se/media/45159/the_etical_review_act.pdf>. [Accessed 4. March 2014].

- Swedish Personal Data Act, 1998 [pdf] Available at: <http://www.government.se/content/1/c6/01/55/42/b451922d.pdf>. [Accessed 25. February 2014].

- Tsiavos, Prodromos; Piperidis, Stelios; Gavrilidou, Maria; Labropoulou, Penny; and Patrikakos, Tasos (2013). Deliverable D 4.5.1: Legal Framework. Retrieved 23 June 2014, from: http://www.qt21.eu/launchpad/system/files/deliverables/QTLP-Deliverable-4_5_1_0.pdf

- UK Data Protection Act 1998. Available at: <http://www.legislation.gov.uk/ukpga/1998/29/contents> [Accessed 05 December 2014].

- University of Bristol 2014a. Research Guidelines: section 33 exemption [Internet], University of Bristol. Available at: http://www.bris.ac.uk/secretary/dataprotection/research/guidelines.html, [accessed on June 19 2014.]

- World Intellectual Property Organization. Berne Convention for the Protection of Literary and Artistic Works. Avaliable at: http://www.wipo.int/treaties/en/text.jsp?file_id=283698. [Accessed on June 23 2014.]

- World Medical Association (WMA) Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects. Available at: http://www.wma.net/en/30publications/10policies/b3/. [accessed on November 23 2014.]

- Wright, J. and J.Terstegge.2004. The Implementation of Directive 95/46/EC in Dutch Law and Medical Research. In: D. Beyleveld, D. Townend, S. Rouille-Mirza and J. Wright, ed. 2004. Implementation of the Data Protection Directive in Relation to Medical Research in Europe. Ashgate. pp. 273-288.

Appendix 1: Country wise table of legal requirements for the processing of personal data within SSH

Here you will find an overview of approval- and notification requirements in the countries presented in this handbook, for the processing of personal data and sensitive personal data.

Country	Sensitive personal data	Non-Sensitive Personal Data
Denmark		
Approval from Data Protection Authority	Yes Exemption if student-thesis based on consent	No
Approval from ethics committee	No	No
Notification requirement	No	No
Estonia		
Approval from Data Protection Authority	Yes, or: appointed Data Protection Officer	No
Approval from ethics committee	In addition if: not based on consent	No
Notification requirement	No	No

Finland		
Approval from Data Protection Authority	No	No
Approval from ethics committee	Recommended if: special issues (e.g. not based on consent)	
Notification requirement	Yes	If: personal data is outsourced or transferred to outside the EU/EEA
Germany		
Approval from Data Protection Authority	If not based on consent, approval from appointed Data Protection Officer (mandatory)	No
Approval from ethics committee	No	No
Notification requirement	If based on consent, notification to appointed Data Protection Officer (mandatory)	Yes

Iceland		
Approval from Data Protection Authority	If involving special privacy risks (e.g. not based on consent)	No
Approval from ethics committee	No	No
Notification requirement	Yes	Yes
Netherlands		
Approval from Data Protection Authority	If involving special privacy risks (e.g. not based on consent)	No
Approval from ethics committee	No	No
Notification requirement	Research are by large exempted from notification requirement, if directly identifying data are deleted within 6 months	Research are by large exempted from notification requirement, if directly identifying data are deleted within 6 months

Norway		
Approval from Data Protection Authority	Yes, either by the Authority or by an appointed data protection officer (depending on scale and duration)	No
Approval from ethics committee	No	No
Notification requirement	No	Yes
Spain		
Approval from Data Protection Authority	Yes	No
Approval from ethics committee	No	No
Notification requirement	No	Yes
Sweden		

Approval from Data Protection Authority	No	No
Approval from ethics committee	Yes	No
Notification requirement	No	To appointed Data Protection Officer if not based on consent
UK		
Approval from Data Protection Authority	No	No
Approval from ethics committee	No	No
Notification requirement	Sufficient with a yearly notification including all the processing of personal data conducted at an institute	Sufficient with a yearly notification including all the processing of personal data conducted at an institute

Appendix II: List of Ethical Boards in Europe

In what follows you may find a list of relevant ethical boards in Europe, classified by country. Most of them refer to Ethical Boards concerned with medical and biological research, but in some cases more general boards are found. You may also find it useful to consult the European Network of Research Ethics Committees (EUREC).

Country	Ethical Board
Austria	Forum of the Austrian Ethics Committees. 26 ethics committees belong to it and use and accept the forms and guidelines distributed by the forum. Link: http://www.ethikkommissionen.at/ (in German only)
Belarus	National Bioethics Committee of the Republic of Belarus.
Belgium	Belgian Advisory Committee on Bioethics Link: http://www.health.belgium.be/eportal/Healthcare/Consultativebodies/Committees/Bioethics/
Bulgaria	Bulgarian Central Ethic Committee
Croatia	Central Ethics Committee Link: http://www.almp.hr/?ln=en&w=o_SEPu
Cyprus	Cyprus National Bioethics Committee-CNBC. It is responsible for the bioethical review of all research protocols involving human subjects in Cyprus. Link: http://www.bioethics.gov.cy/ (in Greek and English)
Czech Republich	Forum of the Czech Ethics Committees. Link: http://www.forumek.cz/ (in Czech only)
Denmark	Danish National Committee on Biomedical Research Ethics. Link: http://www.cvk.sum.dk/ (in Danish and English)
Estonia	Research Ethics Committee of the University of Tartu Link: http://www.eetikakeskus.ut.ee/en/research-ethics-committee-university-tartu-0 (in English) Tallinn Ethics Committee On Medical Research Link: http://www.tai.ee/en/about-us/tallinn-medical-research-ethics-commitee (in English)
Finland	National Committee on Medical Research Ethics Link: http://www.tukija.fi/en/ (in English) National Advisory Board on Research Ethics: Link: http://www.tenk.fi/en/ (in English, Finnish and Swedish)

	Additionally, there are regional research ethics committees established by the University hospital districts.
France	National Consultative Ethics Committee for health and life sciences. Link: http://www.ccne-ethique.fr/ (in French and English) Additionally, there are 39 Ethics Committes in France.
Germany	National Council for Ethics. Link: http://www.ethikrat.org/ (in German and English) German Reference Centre for Ethics in the Life Sciences Link: http://www.drze.de/ (in German and English) Additionally, there are 53 research ethics committees.
Greece	National Bioethics Commission Link: http://www.bioethics.gr/index.php?category_id=3 (in Greek and English) National Ethics Committee of the National Organization for Medicines. Additionally, there are local Research Ethics Committees in hospitals, research centres and higher education institutions.
Hungary	Central Clinico-Pharmacological Ethics Committee. Additionally, each institution taking part in human experiments must have an Institutional Ethics Committee.
Ireland	There are 12 Research Ethics Committees. These must be recognised by the Ethics Committees Supervisory Body. Irish Council for Bioethics.
Italy	Italian National Bioethics Committee Link: http://www.governo.it/bioetica/eng/ (in Italian and English) Consiglio Nazionale delle Richerche, Commissione di Bioetica Link: http://www.cnr.it/ethics/commissione.php (in Italian and English, partially)
Latvia	Central Medical Ethics Committee of Latvia
Lithuania	Lithuanian Bioethics Committee Link: http://bioetika.sam.lt/index.php?-1876243809 (in Lithuanian and English)
Luxembourg	Comité National d'Ethique de Recherche Link: http://www.cner.lu/ (in French, German and English) Commission Nationale d'Ethique Link: http://www.cne.public.lu/ (in French)
Malta	Bioethics Consultative Committee Link: https://ehealth.gov.mt/healthportal/others/regulatory_councils/bioethics_committee/bioethics_committee_home_page.aspx (in English)
Netherlands	There are 12 Research Ethics Committees and a Central Committee responsible for the accreditation of the accredited research ethics committees. Central Committee on Research Involving Human Subjects Link: http://www.ccmo.nl/ (in Dutch and English) Dutch Association of Medical Research Ethics Committees

	Link: http://www.nvmetc.nl/ (in Dutch)
Norway	The Norwegian National Research Ethics Committees Link: https://www.etikkom.no/ (in Norwegian and English) There are three national committees: - The National Committee for Medical Research Ethics (NEM) - The National Committee for Research Ethics in Science and Technology (NENT) - The National Committee for Research Ethics in the Social Sciences and the Humanities (NESH)
Poland	There are 53 Bioethics Committees in Poland. A list of them together with available links can be found here.
Portugal	National Authority of Medicines and Health Products National Ethics Committee for Clinical Research Link: http://www.ceic.pt/portal/page/portal/CEIC (in Portuguese and English) National Data Protection Authority Links: http://www.cnpd.pt/ (Portuguese) http://www.cnpd.pt/english/index_en.htm (English)
Romania	Comité National Roumain de Bioéthique
Russia	Russian Committee for Bioethics Link: http://www.bioethics.ru/eng/rucommittee/ (in English)
Slovakia	Ethics Committee at the Ministry of Health of the Slovak Republic Link: http://www.health.gov.sk/?eticka-komisia (in Slovak) A list of ethical committees together with their contact information can be found here.
Slovenia	National Medical Ethics Committee Link: http://www.kme-nmec.si/ (in Slovenian and English)
Spain	Asociación Nacional de Comités de Ética de la Investigación Link: http://www.ancei.es/ (in Spanish) Spanish Bioethics Committee Link: http://www.comitedebioetica.es/ (in Spanish and English)
Sweden	The Swedish National Council on Medical Ethics Link: http://www.smer.se/ (in Swedish and English) Ethical vetting Link: http://www.epn.se/ (in Swedish and English)
Switzerland	Swiss National Advisory Commission on Biomedical Ethics Link: http://www.nek-cne.ch/?langId=2 (in German, English, French and Italian) Federal Ethics Committee on Non-Human Biotechnology Link: http://www.ekah.admin.ch/en/index.html (in English, French, German and Italian) Swiss Ethics Committees on research involving humans Link: http://www.swissethics.ch/ (in English, French, German and Italian)
United Kingdom	National Research Ethics Service Link: http://www.hra.nhs.uk/ (in English)

	Association for Research Ethics Link: http://www.arec.org.uk/ (in English) Nuffield Council on Bioethics. Link: http://nuffieldbioethics.org/ (in English) Human Fertilisation and Embryology Authority Link: http://www.hfea.gov.uk/ (in English) COREC Link: http://corec.org.uk/ (in English)

List of National Data Protection Authorities in Europe

Here you will find a list of National Data Protection Authorities in Europe. You may also find it useful to consult the European Commission.

Country	National Data Protection Authority
Austria	Österreichische Datenschutzbehörde e-mail: dsb@dsb.gv.at
Belgium	Commission de la protection de la vie privée e-mail: commission@privacycommission.be
Bulgaria	Commission for Personal Data Protection e-mail: kzld@cpdp.bg
Croatia	Croatian Personal Data Protection Agency e-mail: azop@azop.hr or info@azop.hr
Cyprus	Commissioner for Personal Data Protection e-mail: commissioner@dataprotection.gov.cy
Czech Republic	The Office for Personal Data Protection e-mail: posta@uoou.cz
Denmark	Datatilsynet e-mail: dt@datatilsynet.dk
Estonia	Estonian Data Protection Inspectorate e-mail: viljar.peep@aki.ee
Finland	Office of the Data Protection e-mail: tietosuoja@om.fi

France	Commission Nationale de l'Informatique et des Libertés
Germany	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit e-mail: poststelle@bfdi.bund.de
Greece	Hellenic Data Protection Authority e-mail: contact@dpa.gr
Hungary	Data Protection Commissioner of Hungary e-mail: peterfalvi.attila@naih.hu
Ireland	Data Protection Commissioner e-mail: info@dataprotection.ie
Italy	Garante per la protezione dei dati personali e-mail: garante@garanteprivacy.it
Latvia	Data State Inspectorate e-mail: info@dvi.gov.lv
Lithuania	State Data Protection e-mail: ada@ada.lt
Luxembourg	Commission nationale pour la protection des données e-mail: info@cnpd.lu
Malta	Office of the Data Protection Commissioner e-mail: commissioner.dataprotection@gov.mt
The Netherlands	College bescherming persoonsgegevens Dutch Data Protection Authority e-mail: info@cbpweb.nl
Norway	Datatilsynet e-mail: postkasse@datatilsynet.no

Poland	The Bureau of the Inspector General for the Protection of Personal Data e-mail: sekretariat@giodo.gov.pl
Portugal	Comissão Nacional de Protecção de Dados e-mail: geral@cnpd.pt
Romania	The National Supervisory Authority for Personal Data Processing e-mail: anspdcp@dataprotection.ro
Slovakia	Office for Personal Data Protection of the Slovak Republic e-mail: statny.dozor@pdp.gov.sk
Slovenia	Information Commissioner e-mail: gp.ip@ip-rs.si
Spain	Agencia de Protección de Datos e-mail: internacional@agpd.es
Sweden	Datainspektionen e-mail: datainspektionen@datainspektionen.se
United Kingdom	The Information Commissioner's Office E-mail: International.Team@ico.org.uk

Appendix III: Checklist for research projects dealing with sensitive and/or copyrighted data

Prior to carrying out a research project dealing with sensitive and/or copyrighted data, several issues have to be taken into account. What follows is an attempt of providing you with a checklist of issues to be considered.

- Do the project objectives and/or methods break the accepted ethical principles?
- Do you know the relevant ethical board or committee in your country?
- Does the legislation in your country require ethical approval of research projects? If so, did you obtain it?
- Projects involving humans:
    - Did you get the informed consent from the subjects of the experiments?
    - Is there any dependent relationship that could affect such consent?
- Projects involving personal data:
    - Has all personal data been properly anonymised to guarantee the protection of privacy?
- Projects involving copyrighted works:
    - Have all copyright issues been cleared?
    - Does your country have any laws as regards the research and data mining of copyrighted works? If so, are these being complied with in the research project?
    - If you have to clear copyright prior to gathering data, have all copyright holders been contacted and have they sent their consent? What kind of research are you entitled to do?

- Is there a licensing strategy already in place?
- Will the resource be deposited in a repository? If so, has it been negotiated with the repository the conditions that shall apply to the resource?

Appendix IV: Glossary

Term	Definition
Consent of the Data Subject	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 (Article 2 h, Directive 95/46/EC).
Copyright	Copyright is a legal right that grants the creator of an original work exclusive rights, usually for a limited time, to make copies, perform, license or otherwise exploit a work.
Data Controller	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 (Article 2 d, Directive 95/46/EC).
Data Processor	A natural or legal person, public authority,

	agency or any other body which processes personal data on behalf of the controller (Article 2 e, Directive 95/46/EC).
Data Protection Authority	Authorities and institutions dealing with data protection on national or European level.
Data Protection Officer/ Data Protection Official	An officer that independently ensures the application of data protection conducted in a given institution on behalf of the Data Protection Authority.
Intellectual Property Rights (IPRs)	Rights granted to creators and owners of works that are the result of human intellectual creativity. The main intellectual property rights are: copyright, patents, trademarks, design rights, protection from passing off, and the protection of confidential information. (Andrew Charlesworth (2012): Intellectual Property Rights for Digital Preservation)
Personal Data	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 (Article 2 a, Directive 95/46/EC).

Processing of Personal Data	Any operation or set of operations which is performed upon personal data, 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 (Article 2 b, Directive 95/46/EC).
Recipient	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 (Article 2 g, Directive 95/46/EC).
Sensitive Personal Data	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 (referred to as "special categories of data cf. Article 8) 1, Directive 95/46/EC).
Third Party	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 (Article 2 f, Directive 95/46/EC).
Deposition license agreement (DELA)	An agreement between the *repository* and the *owners* of the rights to a deposited resource. It regulates the conditions under which the resource will be made available.
End user license agreement (EULA)	An agreement between the *repository* and the end *users* of a deposited resource. It regulates the conditions under which the users can access and exploit the resource.
Terms of service agreement (TOS)	Terms of use which are not specific to a particular resource, but which apply for all repository services.
Creative Commons	Creative Commons is a nonprofit organisation that provides copyright licenses, which modify the copyright terms to accommodate to the needs of the copyright owner. They are simple and standardised. (http://creativecommons.org)
Copyright owner	Person who owns the copyright of a work because he/she is the creator of such work.
Copyrighted work	Work which is protected by copyright