# D2.4 Legal and Ethical Requirements

<table>
<thead>
<tr>
<th><strong>Type (distribution level)</strong></th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contractual date of Delivery</strong></td>
<td>30.05.2017</td>
</tr>
<tr>
<td><strong>Actual date of delivery</strong></td>
<td>30-06-2015 (updated on 17/02/2017)</td>
</tr>
<tr>
<td><strong>Deliverable number</strong></td>
<td>D2.4</td>
</tr>
<tr>
<td><strong>Deliverable name</strong></td>
<td>Legal and Ethical Requirements</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>2.0 (resubmission upon recommendations of the mid-project review)</td>
</tr>
<tr>
<td><strong>Number of pages</strong></td>
<td>83</td>
</tr>
<tr>
<td><strong>WP/Task related to the deliverable</strong></td>
<td>T2.3</td>
</tr>
<tr>
<td><strong>WP/Task responsible</strong></td>
<td>KUL</td>
</tr>
<tr>
<td><strong>Author(s)</strong></td>
<td>Pieter-Jan Ombelet and Damian Clifford; Stephanie Mihail</td>
</tr>
<tr>
<td><strong>Partner(s) Contributing</strong></td>
<td>N.A.</td>
</tr>
<tr>
<td><strong>Document ID</strong></td>
<td>CLARUS-D2.4-LegalandEthicalRequirements-v2.0</td>
</tr>
<tr>
<td><strong>Abstract</strong></td>
<td>This deliverable provides a detailed analysis of the legal and ethical requirements relevant to the CLARUS solution, with particular emphasis on the privacy and data protection considerations.</td>
</tr>
</tbody>
</table>
Disclaimer

CLARUS (644024) is a Research and Innovation Actions project funded by the EU Framework Programme for Research and Innovation Horizon 2020. This document contains information on CLARUS core activities, findings and outcomes. Any reference to content in this document should clearly indicate the authors, source, organisation and publication date. The content of this publication is the sole responsibility of the CLARUS consortium and cannot be considered to reflect the views of the European Commission.
Executive summary

Although cloud computing has been part of the digital landscape for some time it is only in recent years that the full potential is starting to be realised and exploited. This deliverable aims to analyse the applicable legal and ethical framework and derive the legal requirements relevant to CLARUS and to provide guidance on their implementation in order to ensure the development of a legally compliant solution.

From the analysis provided in this deliverable detailed legal and ethical requirements have been outlined and applied to the context of the application cases thereby distilling applied requirements resulting in the creation of guidelines for the implementation of a legally compliant CLARUS solution. To conclude the work completed it should be noted that in order for the implementation of a legally compliant CLARUS solution, partners must give detailed consideration to the obligations outlined in this report. These specified requirements will form the continuing basis of KUL’s work in Task 6.2 ‘Guidance on compliance with legal obligations’ and more specifically D6.3 ‘Legal assessment and recommendations’.
Table of Contents

1 INTRODUCTION ................................................................................................................. 6

1.1 SCOPE OF THE DOCUMENT ........................................................................................ 6

1.2 REVISION HISTORY ....................................................................................................... 7

1.3 NOTATIONS, ABBREVIATIONS AND ACRONYMS ..................................................... 7

2 CLOUD COMPUTING IN THE CLARUS CONTEXT ................................................................. 9

2.1 BUSINESS MODELS AND ESTABLISHING TRUST AND OWNERSHIP ....................... 9

2.2 THE RESPECTIVE DATA SETS AND THE ASSOCIATED REQUIREMENTS .................... 10

2.2.1 ACCESS directive ..................................................................................................... 11

2.2.2 INSPIRE directive .................................................................................................... 12

2.2.3 PSI re-use framework .............................................................................................. 13

2.3 CONCLUSION .................................................................................................................. 14

3 PRIVACY AND DATA PROTECTION FRAMEWORK .......................................................... 15

3.1 EUROPEAN CONVENTION ON HUMAN RIGHTS ....................................................... 15

3.2 CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION ....................... 16

3.3 DATA PROTECTION DIRECTIVE 95/46/EC ............................................................... 16

3.3.1 Scope of application of EU data protection law ......................................................... 17

3.3.2 Legal grounds for processing of personal data ......................................................... 22

3.3.3 Legal grounds for processing of sensitive data ....................................................... 25

3.3.4 Legal requirements for processing of personal data ................................................ 25

3.3.5 Data subject rights .................................................................................................... 27

3.4 E-PRIVACY DIRECTIVE 2002/58/EC ............................................................................ 30

3.4.1 Applicable provision analysis .................................................................................. 30

3.5 PROPOSED DATA PROTECTION REGULATION ......................................................... 32

3.5.1 Scope of the regulation ............................................................................................ 32

3.5.2 Key proposed changes ............................................................................................ 33

3.6 CONCLUSION .................................................................................................................. 39

4 SECURITY, BREACH NOTIFICATION AND CONTRACTUAL MITIGATION OF LIABILITY ......... 40

4.1 PROTECTING INTEGRITY AND AUTHENTICITY OF CONFIDENTIAL DATA AND GUARANTEEING ACCESS .......................................................... 40

4.2 ENCRYPTION, ANONYMISATION - HOLDING THE KEYS TO PERSONAL DATA ACCESS ........................................................................................................... 40

4.3 BREACH NOTIFICATION OBLIGATIONS ....................................................................... 41

4.3.1 Electronic communication networks and services .................................................... 42

4.3.2 Proposed breach notification obligations .................................................................... 43

© CLARUS Consortium
4.4 CLOUD SERVICE PROVIDER LIABILITY ................................................................. 43
  4.4.1 Contractual mitigation of liability ............................................................. 43
  4.4.2 Negligence - tort liability ....................................................................... 43

4.5 CONCLUSION ............................................................................................... 44

5 LIABILITY OF INTERMEDIARIES ........................................................................ 45
  5.1 EU regime on liability of intermediaries .................................................... 45
    5.1.1 Liability exemptions for intermediaries ................................................. 46
  5.2 Applicability of the hosting exemption on a cloud service provider ........ 51
  5.3 CONCLUSION ............................................................................................... 51

6 PUBLIC SECTOR ACCESS TO CLOUD DATA .................................................. 52
  6.1 Cloud challenges and forensic investigations ............................................ 52
  6.2 Convention on Cybercrime ....................................................................... 53
  6.3 Directive 2013/40/EU on attacks against information systems ............... 55
  6.4 Directive 2014/41/EC on the European Investigation Order in criminal matters .......................... 56
  6.5 CONCLUSION ............................................................................................... 57

7 LEGAL AND ETHICAL REQUIREMENTS TABLE ..................................... 58

8 IMPACT OF REQUIREMENTS ON CLARUS AS DERIVED FROM THE USE CASES ........................................................................ 62
  8.1 Geographic Data Application Case ......................................................... 62
  8.2 eHealth Data Application Case .............................................................. 64
  8.3 Legal Requirements for Governmental Entities ........................................ 65
  8.4 CONCLUSION ............................................................................................... 74

9 IMPLEMENTATION GUIDELINES .................................................................. 75

10 CONCLUSION ............................................................................................... 77

11 REFERENCES .................................................................................................. 78
  11.1 Legislation ................................................................................................ 78
  11.2 Case Law ................................................................................................ 80
  11.3 Opinions ................................................................................................ 80
  11.4 Publications .............................................................................................. 81
1 Introduction

1.1 Scope of the document

Although cloud computing has been part of the digital landscape for some time it is only in recent years that the full potential is starting to be realised and exploited. The purpose of CLARUS is to enhance trust in cloud computing services by developing a secure framework for the storage and processing of data outsourced to the cloud that allows end users to monitor, audit and retain control of the stored data without impairing the functionality and cost-saving benefits of cloud services. This deliverable aims to analyse the applicable legal and ethical framework and derive the legal requirements relevant to CLARUS and to provide guidance on their implementation in order to ensure the development of a legally compliant solution. Moreover, this deliverable considers the project reviewers’ comments regarding the need for refining the implementation guidelines proposed in the first version.

For this deliverable, primary and secondary sources of EU law were used. The relevant legislation, case law and doctrine was selected based on the scope and goals of the CLARUS project. This desktop research focuses on EU frameworks as this is the focus of the description of work.

With this in mind Chapter 2 first provides an analysis of cloud computing in the context of CLARUS in order to derive preliminary legal concerns before the requirements associated with the data sets to be used in the project, as described in D2.1 ‘Definition of application cases’, are outlined.

Chapter 3 gives a detailed analysis of the privacy and data protection framework and requirements, the importance of which is emphasised in the description of work. This includes a detailed outline of Directive 95/46/EC and Directive 2002/58/EC and the proposed modifications as provided for by the Proposed Data Protection Regulation.

Chapter 4 examines the security specific requirements and in particular breach notification obligations and contractual mitigation of liability

Chapter 5 outlines the requirements in relation to the liability of intermediaries and Chapter 6 describes the issues in relation to public authority access to cloud data.

Following this analysis the extrapolated requirements are presented in a requirements table in Chapter 7 before being applied to the context of the project in Chapter 8 Impact on CLARUS. This analysis relies on D2.1 ‘Definition of application cases’. As such, for a thorough examination of the use cases reference should be made to D2.1. Chapter 9 transposes the requirements into guidelines for their implementation into the CLARUS solution.

Finally Chapter 10 concludes the analysis.
1.2 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>11/03/2015</td>
<td>Damian Clifford</td>
<td>Draft table of contents</td>
</tr>
<tr>
<td>0.2</td>
<td>15/05/2015</td>
<td>Pieter-Jan Ombelet and Damian Clifford</td>
<td>Internal draft of the deliverable</td>
</tr>
<tr>
<td>0.3</td>
<td>02/06/2015</td>
<td>Pieter-Jan Ombelet and Damian Clifford</td>
<td>Draft deliverable</td>
</tr>
<tr>
<td>0.4</td>
<td>19/06/2015</td>
<td>EURECOM</td>
<td>Review by EURECOM</td>
</tr>
<tr>
<td>0.5</td>
<td>22/06/2015</td>
<td>Pieter-Jan Ombelet and Damian Clifford</td>
<td>Integration of review</td>
</tr>
<tr>
<td>1.0</td>
<td>30/06/2015</td>
<td>Pieter-Jan Ombelet and Damian Clifford</td>
<td>Final version of the deliverable</td>
</tr>
<tr>
<td>2.0</td>
<td>17/02/2017</td>
<td>Stephanie Mihail</td>
<td>Resubmission upon reviewers’</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>recommendations</td>
</tr>
</tbody>
</table>

1.3 Notations, abbreviations and acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>DPD</td>
<td>Data Protection Directive 95/46/EC</td>
</tr>
<tr>
<td>ECD</td>
<td>E-Commerce Directive 2000/31/EC</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights and Fundamental Freedoms</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EIO</td>
<td>European Investigation Order</td>
</tr>
<tr>
<td>ePD</td>
<td>E-Privacy Directive 2002/58/EC</td>
</tr>
<tr>
<td>FOI</td>
<td>Freedom of Information</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>LIBE</td>
<td>European Parliament’s Committee on Civil Liberties, Justice and Home Affairs</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Security</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Cooperation and Development</td>
</tr>
<tr>
<td>PSI</td>
<td>Public Sector Information</td>
</tr>
</tbody>
</table>
2 Cloud computing in the CLARUS context

This chapter of the analysis will provide an outline of the cloud computing services and the data sets relevant to the CLARUS project and thus the associated preliminary legal considerations. This will form the basis for the analysis provided during the rest of this deliverable. Accordingly, the section will examine the data sets to be used in the context of CLARUS and the applicable legal frameworks concerning access.

2.1 Business models and establishing trust and ownership

To begin our analysis, it is perhaps prudent to first briefly assess cloud computing services and business models in order to decipher the relevant legal concerns. In essence, there are three key models of cloud computing namely:

1. Infrastructure as a service (IaaS) which relates to the provision of computing resources e.g. computing power;
2. Platform as a service (PaaS) which concerns the provision of tools for the development of custom applications; and
3. Software as a service (SaaS) which involves application hosting by providers of applications made available to clients over a network.

In the context of CLARUS it appears that the second and third of these categories is the most relevant. CLARUS aims to enhance trust in cloud computing services by developing a secure framework for the storage and processing of data outsourced to cloud services allowing end users the ability to monitor, audit and retain control over the stored data without impairing the functionality and cost-saving benefits of cloud services.

From a legal perspective trust is a difficult concept. Indeed:

“There is no overarching concept of trust in the European legal framework, but elements creating the legal conditions for this trust to occur can be found in legal provisions relating to many different topics.”

In the context of this analysis the report will focus on the data protection and security elements as methods of harnessing trust and also issues related to the liability of intermediaries and public sector access to cloud data. However, before examining these elements it is important to first briefly assess issues related to the ownership of the data and interoperability.

Regarding the former of these, it is apparent that the CLARUS solution aims not only at improving the security of data in the context of malicious threats but also against what can be described as “honest but curious” behaviour of the cloud. This has particular relevance in relation to the Cloud Service Providers (CSPs) and their ability to access data stored by cloud users. Given the potential sensitivity of such information users may not find such practices acceptable and the use of the CLARUS solution may somewhat mitigate such fears. However, certain legal issues should be considered in relation to the ownership of data and the cloud contracts offered by certain CSPs. First some cloud providers reserve the right to use the cloud user’s data for their own business interests the extent of which differs depending on the wording of the terms of use. Also associated with this concern is the extent to which the cloud service provider has access to the data for monitoring and maintenance purposes and the purposes for

---

2 Ibid., 39.
which it can use any resulting information.\textsuperscript{3} In relation to the interoperability issue, it is clear that CLARUS may involve the use of multiple cloud service providers simultaneously by one user. This raises interoperability issues from a technical and also potentially from a policy perspective. As a consequence this could result in unreasonable dependencies. CLARUS aims to resolve this issue and as a consequence the linked data portability issue. The data sets to be used in the context of the CLARUS project and any potentially associated requirements will now be considered.

2.2 The respective data sets and the associated requirements

As described in D2.1 ‘Definition of application cases’, the development of CLARUS relies on the use of two distinct data sets namely; geospatial data and eHealth data. D2.1 provides a comprehensive overview of the applications to which the CLARUS solution will be applied during the course of the project and the types of data that will be used. Although this legal deliverable is focused on the privacy and data protection issues associated with the CLARUS solution as it aims to increase the security of data stored on the cloud, the analysis will first briefly outline the applicable rules regarding the availability of this data. In general, access to information held by the public sector is dictated by national freedom of information (FOI) laws. Indeed, at an EU level this is dominated by the principle of subsidiarity which stipulates that “in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.”\textsuperscript{4}

Moreover, FOI legislation generally provides an exemption on the release of information containing personal data without the consent of the data subject in order to comply with data protection and privacy rules.\textsuperscript{5} Accordingly, in relation to health data the security and confidentiality of health records is paramount.

Despite this general disparity in FOI law there are two clear exceptions regarding access related to environmental and spatial data which have particular significance in relation to the geospatial data being used during the CLARUS project. Indeed as described in D2.1, the EU has established a clear legal framework vis-à-vis the availability of public sector spatial data. These European initiatives have three Directives at their core namely:

- Directive 2003/4/EC on public access to environmental information (ACCESS Directive);\textsuperscript{6}
- Directive 2007/2/EC establishing an Infrastructure for Spatial Information in the European Community (INSPIRE Directive);\textsuperscript{7}
- Directive 2003/98/EC on the re-use of public sector information L 345/90 as amended by Directive 2013/37/EU (PSI Re-use Framework).\textsuperscript{8}

Each of these frameworks will now be assessed in order to provide a detailed understanding of any potential \textit{de facto} requirements that may stem from their provisions.

\begin{footnotesize}
\begin{enumerate}
\item Ibid., 39.
\item Article 5(3) TEU.
\item Also Ireland for example extends this to deceased persons who are not protected under data protection provisions.
\end{enumerate}
\end{footnotesize}
2.2.1 ACCESS directive

According to Article 3 of Directive 2003/4/EC:

“Member States shall ensure that public authorities are required, in accordance with the provisions of this Directive, to make available environmental information held by or for them to any applicant at his request and without his having to state an interest.”

From this Article the Directive requires public bodies to make environmental information available to the public either through express public request or proactively of their own initiative. As such this ensures that citizens are able to access environmental data in order to participate and assess the governmental decision making process. From Article 3(4) public authorities are required to supply information in the format requested by the applicant unless:

“(a) it is already publicly available in another form or format, in particular under Article 7, which is easily accessible by applicants; or
(b) it is reasonable for the public authority to make it available in another form or format, in which case reasons shall be given for making it available in that form or format.”

This provision goes on to state that public authorities are required to make “all reasonable efforts” to maintain the information in formats easily accessible “by computer telecommunications or by other electronic means.”

This sentiment is also reflected in Article 4(1) which encourages the dissemination of information as much as possible through information technology means but does not explicitly require the conversion of information into an electronic form. Article 7(2) provides a list of the minimum amount of information that must be made available. This states that “[t]he information to be made available and disseminated shall be updated as appropriate and shall include at least:

(a) texts of international treaties, conventions or agreements, and of Community, national, regional or local legislation, on the environment or relating to it;
(b) policies, plans and programmes relating to the environment;
(c) progress reports on the implementation of the items referred to in (a) and (b) when prepared or held in electronic form by public authorities;
(d) the reports on the state of the environment referred to in paragraph 3;
(e) data or summaries of data derived from the monitoring of activities affecting, or likely to affect, the environment;
(f) authorisations with a significant impact on the environment and environmental agreements or a reference to the place where such information can be requested or found in the framework of Article 3;
(g) environmental impact studies and risk assessments concerning the environmental elements referred to in Article 2(1)(a) or a reference to the place where the information can be requested or found in the framework of Article 3.”

This list is non-exhaustive and hence Member States are permitted to add additional elements. As a result national implementations need to be consulted in order for a precise and definitive list in relation to a particular jurisdiction.

In the context of CLARUS, it is significant to note the exception from this general right of access as provided for in Article 4. These are split into formal administrative exemptions and those based on content. The

---

9 K. Janssen, The EC Legal Framework for the Availability of Public Sector Spatial Data: An examination of the criteria for applying the directive on access to environmental information, the PSI directive and the INSPIRE directive, Doctoral dissertation in law, 4 December 2009, KU Leuven, 18-19.
latter of these groupings has a clear effect on the CLARUS solution in relation to the application to the geospatial data context as such content exceptions will require security protections against unauthorised access. Accordingly, Article 4(2) stipulates that:

“Member States may provide for a request for environmental information to be refused if disclosure of the information would adversely affect:
(a) the confidentiality of the proceedings of public authorities, where such confidentiality is provided for by law;
(b) international relations, public security or national defence;
(c) the course of justice, the ability of any person to receive a fair trial or the ability of a public authority to conduct an enquiry of a criminal or disciplinary nature;
(d) the confidentiality of commercial or industrial information where such confidentiality is provided for by national or Community law to protect a legitimate economic interest, including the public interest in maintaining statistical confidentiality and tax secrecy;
(e) intellectual property rights;
(f) the confidentiality of personal data and/or files relating to a natural person where that person has not consented to the disclosure of the information to the public, where such confidentiality is provided for by national or Community law;
(g) the interests or protection of any person who supplied the information requested on a voluntary basis without being under, or capable of being put under, a legal obligation to do so, unless that person has consented to the release of the information concerned;
(h) the protection of the environment to which such information relates, such as the location of rare species.”

It must be acknowledged that these exceptions are optional and Member States are free to choose whether they implement them in their national legislation. As a result, this permits a level of disparity in relation to the application of this framework across the Member States.

Furthermore, these content related exemptions for refusal can only be invoked if the disclosure of the information would “adversely affect” the interests that are protected and they must be interpreted in a restrictive way in a balancing of the respective interests. Given the particular focus of this deliverable (and indeed CLARUS more broadly) on the protection of personal data it is important to observe that an additional safeguard is added. Indeed Article 4(2) goes on to state that even if this balancing test finds in favour of disclosing environmental information containing personal data:

“Member States shall ensure that the requirements of 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 are complied with”

Finally, Article 4(4) provides that where possible information containing elements protected by an exemption should be separated so that the remaining information may be made public.

2.2.2 INSPIRE directive

Directives 2007/2/EC establishes a legal basis for the creation of the Infrastructure for Spatial Information in the European Community (INSPIRE). This requires the exchange of spatial data between public authorities regarding the performance of public tasks related to the environment and to facilitate the public access. Accordingly, the key focus of the INSPIRE Directive is on sharing and the availability of spatial data for public tasks which may have an impact on the environment. There is therefore a clear overlap with the ACCESS Directive, which is addressed in Article 2 of the Directive 2007/2/EC. The Article stipulates

10 K. Janssen, l.c., 84.
that where the ACCESS and INSPIRE Directives would have irreconcilable provisions the former will prevail. The provisions of the INSPIRE Directive will however apply as long as they remain within the margins left by the ACCESS Directive.\(^{11}\)

It should be noted that the INSPIRE framework creates detailed rules on the availability of high quality metadata for all data sets and services. This is provided in Article 5(2) of the INSPIRE Directive which provides that

"Metadata shall include information on the following:
(a) the conformity of spatial data sets with the implementing rules provided for in Article 7(1);
(b) conditions applying to access to, and use of, spatial data sets and services and, where applicable, corresponding fees;
(c) the quality and validity of spatial data sets;
(d) the public authorities responsible for the establishment, management, maintenance and distribution of spatial data sets and services;
(e) limitations on public access and the reasons for such limitations, in accordance with Article 13."

Article 5(2)(a) refers to the specific conditions set out by the Commission Regulation in relation to the particular metadata elements that must be included and the instructions on how these must be included and described.

For the purposes of this analysis it is clear that the limitations on access to the network services to be provided under the Directive as established by Article 11 are a key consideration. Article 13(1) provides a list of derogations that may limit the public access to data sets and services as provided by the network services. From the above these are also to be provided in the metadata (see Article 5(2)(e)). These limits are split in two between those provided for discovery and other services. Regarding the former, public access can only be limited “where such access would adversely affect international relations, public security or national defence.” Accordingly, it is clear that this exemption can only be invoked for severe reasons. In contrast other services can be limited for additional reasons. In essence, these additional limitations are the same as those provided under the terms of the ACCESS Directive. As such, reference can be made to the list provided supra. Also similar to the ACCESS Directive these limitations must be interpreted narrowly and accordingly a balance must be struck between the competing interests.

2.2.3 PSI re-use framework

Directive 2003/98/EC as amended by Directive 2013/37/EU provides the framework for the reuse of public sector information and provides the minimum rules for public authorities to make their data available for commercial or non-commercial reuse without establishing a general right of access. The adoption of the PSI Directive (Directive 2003/98/EC) was the culmination of the Commission’s efforts in encouraging reuse. Fundamentally, the framework is designed to stimulate the European information services market. In 2010, the Commission began a public consultation process measuring the effect of the 2003 Directive.\(^{12}\) The results indicated that although there had been considerable progress made, certain barriers were still preventing the realisation of the full potential of PSI re-use. As a result the Directive was amended in 2013 by Directive 2013/37/EU and Member States are required to implement the changes by the 18th of July 2015.

---

\(^{11}\) K. Janssen, l.c., 92.
The fundamental criticism of the PSI framework relates to the lack of EU competence to require a right of access in the Member States. This reflects the fact that this is an area of joint competence, and is thus dictated by the principle of subsidiarity. As outlined supra EU Member States have guarded their authority over FOI and access tightly and essentially decide which data sets become public. To exacerbate the shared competence issue under the 2003 process, not only did the Member States decide on the types of information the public had access to, they were also permitted to further decide on the publicly available information which could be re-used. The 2013 amendments have addressed this issue and Public Sector Bodies are now required to allow re-use, for non-commercial purposes, of existing and generally available PSI.

There are two important stipulations on this right to non-commercial re-use which also potentially present a challenge. The first is the interaction between Intellectual property rights and the PSI framework. In the 2003 Directive, recitals 22 and 24 briefly mention the issue of intellectual property rights. From these, it is clear that the intellectual property rights of third parties are not to be affected by the 2003 Directive. A second stipulation as provided by the 2013 Amendments is that the re-use of PSI cannot breach the data protection legislation.

### 2.3 Conclusion

From the above introductory analysis it is clear that a key concern relates to the access rights to the stored data sets. In the context of CLARUS this refers to the secure storage and processing of data and the authentication procedures regarding data access to information outsourced to CSPs. In the relevant contexts for the project (namely geospatial data and eHealth data) different degrees of access and associated rights need to be catered for in the design of the CLARUS solution. More particularly as specified in relation to the geospatial data certain information can be made public and other elements have restricted access rights. Accordingly this is significant for the design of the CLARUS solution so that such data classifications are catered for and respected.

---

13 See recitals 22 and 24.
3 Privacy and data protection framework

CLARUS has a clear focus on the privacy and data protection issues as specified by the aims of the project. This Chapter provides an analysis of the current and proposed data protection and privacy framework in order to decipher the key legal requirements. These requirements are relevant for the implementation of a legally compliant CLARUS solution. A particular focus is given for the concept of Privacy by Design and the associated challenges for the implementation of such an approach.

3.1 European Convention on Human Rights

Privacy regulations have only become widely accepted since the second half of the 20th century. The 1948 United Nations Universal Declaration of Human Rights first recognised privacy as a fundamental right. Public concern related to this fundamental right have since grown with the rise of the new information age.

Within Europe the main privacy provision can be found in Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR), concluded in 1950 in the framework of the Council of Europe. This general provision on the right to respect for private and family life is stated as follows:

“1. Everyone has the right to respect for his private life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

The European Court of Human Rights (ECtHR) further clarified these broad terms and emphasised that the concept of private life “extends to aspects relating to personal identity”, such as a person’s name or his or her picture.16 The protection of Article 8 furthermore includes, “beyond a person’s name, other means of personal identification” as well as “the right to establish and develop relationships with other human beings” in professional or business contexts as in others.17

The existing rules with regard to the right to respect one’s private life have continuously been evaluated in the case law of the ECtHR and the national courts, especially in order to address the legal challenges that arise due to the emergence of new technologies.

16 See e.g. ECtHR Friedl v. Austria, 31 January 1995, no. 15225/89; ECtHR Von Hannover v. Germany, 24 June 2004, no. 59320/00; ECtHR Küchl v. Austria, 4 December 2012, no. 51151/06.
3.2 Charter of Fundamental Rights of the European Union

The European Union has also included provisions on the right to respect for privacy as well as an explicit right to protection in the case of personal data processing in the Charter of Fundamental Rights of the European Union (the Charter). The Charter was proclaimed and published in December 2000\(^{18}\) and states in its Articles 7 and 8:

“Article 7 - Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 - Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority”

The Lisbon Treaty formally recognised the binding legal status of the Charter.\(^{19}\) In addition, the Lisbon Treaty provided specific provisions relating to the legal significance of the ECHR. The provisions of the Charter shall hence be applied in conformity with Article 8 ECHR and the interpretation of this Article by the ECtHR.

3.3 Data Protection Directive 95/46/EC

In 1980, the Organisation for Economic Cooperation and Development (OECD) adopted Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.\(^{20}\) These Guidelines aimed to harmonise national privacy legislation to prevent disparities that could hamper the free flow of personal data across frontiers. These guidelines were later followed by the Council of Europe 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention 108”\(^{21}\)). This Convention was the first legally binding international instrument addressing the protection of personal data. As specified by Article 1:

“The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental

\(^{18}\) OJ. C 364/1, 18 December 2000.
\(^{19}\) Article 6 (1) of the Treaty of the European Union (TEU) states in this regard that “[t]he Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union […] which shall have the same legal value as the Treaties.”
freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.”

However, diverging national data protection legislation remained. As a consequence the European Commission proposed the EU Data Protection Directive (DPD). The goal of this Directive was to harmonise and achieve a uniform level of data protection in all the EU Member States in order to facilitate the free flow of data. The DPD clarifies certain privacy principles already outlined in Convention 108 but also offers certain novel general data protection principles that need to be respected when processing personal data. Furthermore, it emphasises that each Member State shall apply their national provisions, after implementing the provisions of the Directive. All Member States have enacted laws implementing the Directive and applying its core principles.

### 3.3.1 Scope of application of EU data protection law

Regarding the scope of application of the EU data protection edifice the analysis is divided between the material scope, the relevant actors and the territorial scope. As such our analysis will be divided accordingly.

#### 3.3.1.1 Material scope

**Personal data**

Under the DPD ‘personal data’ are defined as “information relating to an identified or identifiable natural person”. This relates to information about a person whose identity is either manifestly clear or can be discovered by acquiring additional information. Hence, Article 1 DPD aims to protect the right to privacy of natural persons with respect to the processing of personal data.

The wording ‘any information’ in this definition already hints at a wide interpretation. Regarding the nature of the information, personal data includes any sort of statements about a person. It covers ‘objective’ information, such as the presence of a certain substance in someone’s blood. It also includes ‘subjective’ information, opinions or assessments. The ECtHR has emphasised that personal data is not limited to matters of the private sphere of an individual. The Court of Justice of the European Union (CJEU) stated in this regard that “it is of no relevance that the data published concerns activities of a professional [...] nature from the notion of private life.”

With regard to the format or medium on which the information is contained, ‘personal data’ includes information available in whatever form (alphabetical, numerical, graphical, photographic or acoustic, etc.). It includes information kept on paper, as well as information stored in a computer memory by means of binary code, or on a videotape, for instance. Sensitive data (cf. infra section 3.3.3) is also included under the definition of ‘personal data’.

---

22 Article 4 DPD.
23 For a list of the laws in effect for each member state, see European Commission, Justice and Home Affairs, Data Protection: Status of Implementation, [http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm).
24 Article 2 (a) DPD.
27 ECtHR Amann v. Switzerland, 16 February 2000, no. 27798/95, § 65.
28 CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, § 59.
data’. 30 ‘Personal data’ does not need to be proven or true. When certain information is false or incomplete, every data subject is offered the right to obtain from the controller the rectification, erasure or blocking of this data. 31 Sound and image data (e.g. images of individuals captured by a video surveillance system) are only considered personal data insofar as the individual is recognisable. 32

In general terms, information can be considered to ‘relate’ to an individual when it is about that individual. This is however not a prerequisite for information to be considered ‘personal data’. It has to, at the very least, relate to an identifiable person, i.e. “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”. 33 It is not required to have that individual’s name.

With regard to deceased persons, the Council’s revised draft of the General Data Protection Regulation 34 states that

“The principles of data protection should not apply to deceased persons, unless information on deceased persons is related to an identified or identifiable natural person.”

Processing
The DPD only applies when personal data is being processed. Article 2 (b) DPD defines the processing of personal data as “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”. This definition is deliberately very broad and covers almost all operations (collection, use, destruction, etc.) performed on personal data. The majority of actions performed within the CLARUS project with regard to personal data will therefore be regarded as ‘processing’ in the light of the DPD.

3.3.1.2 Personal scope

Once an action falls within the material scope of the DPD, the next step is to determine which entity (or entities) is (are) responsible for the compliance with its provisions. The key actors within the DPD are the data controller, the data processor and the data subjects.

Data controllers
Article 2 (d) DPD defines a data controller as “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 [...]”. The controller will have to comply with the substantial provisions of the Directive as they are responsible for the processing. The definition has two main elements. First, the DPD references a determinative influence (‘determines’) of each data controller. This natural or legal person decides why certain data is being processed and how this objective shall be reached. 35 This already links to the second

30 Sensitive data is defined in article 8 (1) DPD as “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”. The processing of this data is prohibited unless a specific exception of article 8 (2) DPD applies (e.g. if the sensitive data has to be processed to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent).
31 Article 12 (b) DPD.
33 Article 2 (a) DPD.
component. The controller determines the means and purpose(s) of the processing. For example, a hospital may use patient records for research purposes.\(^{36}\)

The controller can delegate certain organisational or technical matters regarding the means. It is therefore possible that the technical and organisational means are determined exclusively by the data processor.\(^{37}\)

The DPD recognises that a processing activity might be concluded by more than one entity. The definition in Article 2 (d) explicitly covers this possibility of controllers determining the purposes and means “alone or jointly with others”. The joint controllers will then share the subsequent responsibility. There are multiple scenarios possible according to the Article 29 Working Party’s interpretation of the word ‘jointly’. They give the example of a travel agency sending personal data of its customers to airlines and a chain of hotels, to jointly provide a full travel package. These three players will be different data controllers on this common reservation panel, each subject to the data protection provisions relating to its own processing activities.\(^{38}\) Other variations are also possible.


**Data processors**

The processor is defined as “a natural person or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.”\(^{39}\) This definition confirms that the controller decides on its own whether they process the data within their organisation or if they entrust all or part of the processing activities to an external organisation, i.e. the processor. The existence of the processor

\(^{36}\) B. Van Alsenoy, A. Kuczerawy and J. Ausloos, “Search engines after Google Spain: internet@liberty or privacy@peril?”, ICRI Research Paper 15, 6 September 2013, 14.


\(^{38}\) Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, 19.

\(^{39}\) Article 2 (e) DPD.
therefore depends on a decision taken by the controller.\textsuperscript{40} The activities delegated to the processor can be limited to a very specific duty or context or may be rather general and comprehensive.\textsuperscript{41}

It is significant to emphasise that the processor always has to act on behalf of the controller. The processor must only process personal data when and if it receives instructions from the controller.\textsuperscript{42} Secondly, the processor has to guarantee data security when processing data. The controller must, where processing is carried out on its behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out. Furthermore, the controller must ensure compliance with those measures.\textsuperscript{43} The lawfulness of the processor’s data processing activity is determined by the mandate given by the controller. A processor that goes beyond its mandate and acquires a relevant role in determining the purposes or the essential means of processing is a (joint) controller rather than a processor.\textsuperscript{44}

Finally, due to its secondary role, the processor’s responsibility will be lower with regard to its processing activities than the controller, who remains the principal responsible entity. The processor merely needs to guarantee the security of the data by keeping it secure from unauthorised access, disclosure, destruction or accidental loss and follow the delegation of tasks set out by the controller concerning the use of the data.

**Data subjects**

The third entity in the context of the data protection framework is the data subject. This is the person to whom the personal data (directly or indirectly) relates.\textsuperscript{45}

**Personal scope in a cloud computing context**

Determining the rules of the relevant actors in the cloud computing context can sometimes be challenging. Indeed, although CSPs provide the storage capacity, they may not themselves determine the means and purposes of the processing (arguably resulting in a data processor classification). However, in general CSPs will also be considered data controllers, as they often process the personal data stored using their services for purposes such as security and the monetisation of their platforms. Moreover, CSPs also process personal data used for access control mechanisms and authentication protocols. Nevertheless, CSPs are not the only actor which could satisfy the data controller definition. Data providers who adopt CSP solutions clearly also satisfy the data controller definition. In the context of CLARUS, this matter is further complicated given that the project is treating CSPs as “honest but curious” and as a result requiring the encryption of all data. Accordingly CSPs will be prevented from accessing raw data stored using their services. However even in the context of CLARUS, authentication security safeguards will potentially require the processing of personal data, thereby meaning that CSPs adopting the CLARUS solution may also satisfy the data controller definition. Currently this issue remains unclear and is an element which will require detailed monitoring during the implementation of the CLARUS solution. Indeed, currently the form that the CLARUS proxy solution will take remains somewhat unclear. Thus it is uncertain if this solution will fall under the definition of a specific actor or if it will instead form part of a software solution implemented on the CSP and the data provider sides. Finally, it should be noted that in the proposed Data

\begin{itemize}
  \item Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, 1.
  \item Council of Europe, European Agency for Fundamental Rights, l.c., 52.
  \item Article 16 DPD.
  \item Article 17 (2) DPD.
  \item Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, WP 169, 16 February 2010, 25.
  \item Article 2 (a) DPD.
\end{itemize}
Protection Regulation the notions and responsibilities of data controllers and processors are becoming increasingly aligned (cf. *infra* section 3.5).

### 3.3.1.3 Territorial scope

The territorial scope of the DPD is determined by Article 4(1) DPD. This Article states that national provisions adopted pursuant to the Directive shall apply to the processing of personal data where:

“(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.”

Two main criteria can be distilled from this Article. We must take into account (a) the location of the establishment of the controller and (b) the location of the equipment used by the controller for purposes of processing personal data.

Concretely, this means that when an undertaking is established in one or several of the 28 Member States and the processing takes place in the context of the activities of this establishment, the undertaking has to comply with the national law applicable to that establishment. Furthermore, the Article 29 Working Party stresses that the location where the data itself is stored is irrelevant. The only determining factor is whether or not the personal data is processed in the context of activities of a controller established in one or more Member States. Or more specifically, the establishment must perform an “effective and real exercise of activities in the context of which the personal data are being processed.” As an example, let us introduce a company established in Member State A which is collecting data in Member State B. The data are collected in Member State B without an establishment there. The company is only located in Member State A. This data is processed in the context of the activities of the establishment in A. This means that the applicable law will be the law of Member State A.

When an undertaking has an establishment in more than one Member State, one needs to assess in the context of the activities of which establishment the processing has taken place. Therefore, it is possible that different applicable laws apply for different stages of the processing. Nevertheless, “a set of operations carried out in a number of different Member States but all intended to serve a single purpose might well result in the application of a single national law.”

---

47 Ibid., 11.
48 Ibid., 12.
49 Ibid., 12-13.
Most authors and regulators agree that Article 4(1)(a) does not require that the establishment actually acts as a controller, nor that the processing takes place on EU territory. The DPD can therefore have legal implications beyond the territory of the European Economic Area (EEA): the Directive – and national laws of implementation – applies to the processing of personal data outside the EEA (where carried out in the context of activities of an establishment of the controller in the EEA), as well as to controllers established outside the EEA (when they use equipment in the EEA). Therefore, the provisions of the Directive can be applicable to services with an international dimension such as search engines, social networks and CSPs.

Finally, not any use of equipment (or means) within the territory of the EEA leads to the application of the DPD. The concept of ‘making use’ presupposes some kind of activity of the controller and the clear intention of the controller to process personal data. Equipment should therefore receive a broad interpretation, which includes human and/or technical intermediaries, such as in surveys or inquiries.

### 3.3.2 Legal grounds for processing of personal data

Article 7 DPD provides the legal grounds for processing of personal data. It states that personal data may be processed only if:

“(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

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

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

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

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).”

This list is exhaustive. There can be no additional grounds for processing in the national implementations of the Directive.

Article 8 (2) of the Charter specifically recognises consent as the key condition for the processing of personal data. It states that “[s]uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

---


51 Article 29 Working Party, Opinion 8/2010 on applicable law, 8.

52 The notion of “equipment” has been expressed in other official EU languages by the term “means”.

Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”

Article 7 (a) speaks of unambiguous consent by the data subject for the processing. This consent is defined as “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”.  

The key criteria of this concept of consent deserve further exploration. Valid consent has to be:

- **Unambiguous**: For consent to be unambiguous, the procedure to seek and to give consent must leave no doubt as to the data subject's intention to deliver consent. There can be no room for ambiguity or reasonable doubt regarding the data subject’s intent. The Article 29 Working Party summarised in this regard that data controllers are heavily encouraged to foresee procedures or mechanisms that leave no doubt that consent has been given. The minimum expression of an indication could be any kind of signal, sufficiently clear to be capable of indicating a data subject’s wishes, and to be understandable by the data controller. The expression of consent should therefore either be on the basis of an express action carried out by the individual or by being clearly inferred from an action carried out by an individual.

- **Specific**: Consent should be intelligible and refer precisely to a well-defined, concrete situation of data processing. It cannot relate to a non-exhaustive set of processing activities.

- **Freely given**: Consent is freely given as long as the data subject is able to exercise a real choice without risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.

- **Informed**: Article 10 and 11 DPD provide information requirements for the controller. ‘Informed’ consent means consent by the data subject based upon an appreciation and understanding of the facts and implications of an action.

Recital 32 of the Directive further emphasises that data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject has given their explicit consent. However, this explicit consent is currently solely required with regard to the processing of sensitive data. The Proposed General Data Protection Regulation goes one step further and requires that consent given in a written declaration must be distinguishable from any other matter dealt with in the declaration. Safeguards should further ensure that the data subject is aware that and to what extent consent is given. The Regulation also stipulates that consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller (e.g. in the employment sector). Lastly on consent, the Regulation provides for the right of data subjects to withdraw their consent at any time. This withdrawal of consent shall not affect the lawfulness of processing based on a valid consent before its withdrawal.

---

54 Article 2 (h) DPD.
56 Ibid., 11.
57 Ibid., 25.
58 Ibid., 17.
59 Ibid., 12.
61 Article 8 (2) a DPD.
62 Recital 32 and Article 7 (2) of the Regulation.
63 Recital 34 of the Regulation.
64 Article 7 (3) of the Regulation.
The second ground of Article 7 DPD deems processing of personal data lawful when it is “necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.”\(^{65}\) This ground concerns occasions in which a data subject has entered into a contract. This may include, for example, processing the address of the data subject so that goods bought online can be delivered, or processing credit card details in order to finalise payment.\(^{66}\) The second part of this provision covers pre-contractual relations, provided that steps are taken at the request of the data subject, rather than at the initiative of the controller or any third party.\(^{67}\)

Personal data can also be processed if it is “necessary for compliance with a legal obligation to which the controller is subject.”\(^{68}\) There has to be a clear and specific legal obligation in the laws of the EU or one of the Member States. The controller should not have a choice whether or not to fulfil the obligation. Voluntary unilateral engagements and public-private partnerships processing personal data beyond what is required by law are therefore not covered under Article 7(c).\(^{69}\) For example, hospitals often have a legal obligation to store data about the medical history and treatment of patients for several years.\(^{70}\)

As a fourth ground, Article 7 allows processing when it “is necessary in order to protect the vital interests of the data subject.”\(^{71}\) The choice of the wording *vital interest* already suggests that this ground covers a very limited number of situations, applied on a case by case basis. This provision cannot be used normally to legitimise any massive collection or processing of personal data.\(^{72}\) Classical examples of vital interests mostly relate to medical situations or the processing of data about missing persons.

Article 7 (e) DPD refers to the lawful processing if it is “necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.” Article 7(e) covers two situations and is relevant both to the public and the private sector. First, it covers situations where the controller itself has an official authority or a public interest task and he processes personal data in order to exercise that authority or perform that task. Second, Article 7(e) covers situations where the controller does not have an official authority, but is requested by a third party having such authority to disclose data.\(^{73}\)

Lastly, processing personal data can be lawful when it is “necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.” This ground only allows processing when the legitimate interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The legitimate interest of the controller or third party therefore has to prevail the (fundamental rights) interests of the data subject. This entails a balancing exercise on a case-by-case basis.\(^{74}\) In this regard, the CJEU has stated

\(^{65}\) Article 7 (b) DPD.
\(^{67}\) Ibid., 17.
\(^{68}\) Article 7 (c) DPD.
\(^{70}\) Council of Europe, European Agency for Fundamental Rights, l.c., 82.
\(^{71}\) Article 7 (d) DPD.
\(^{73}\) Ibid., 21.
\(^{74}\) Ibid., 23.
in ASNEF and FECEMD\textsuperscript{75} that “Article 7(f) of [the] directive precludes a Member State from excluding, in a categorical and generalised manner, the possibility of processing certain categories of personal data, without allowing the opposing rights and interests at issue to be balanced against each other in a particular case”.\textsuperscript{76}

### 3.3.3 Legal grounds for processing of sensitive data

Article 8 DPD contains a detailed regime for the processing of certain categories of sensitive data. The general rule of this provision prohibits the processing of personal data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”\textsuperscript{77} The legislator has however foreseen certain grounds under which the processing of sensitive data is allowed, i.e. where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.”\textsuperscript{78}

Specifically with regard to medical or health data, Article 8 (3) of the DPD allows for processing of medical data where this is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services. The processing in these cases has to however be done by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

### 3.3.4 Legal requirements for processing of personal data

In the context of CLARUS, it is necessary to discuss the legal requirements for data processing provided in the Directive.

\textsuperscript{75} CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011.

\textsuperscript{76} Para. 48.

\textsuperscript{77} Article 8 (1) DPD.

\textsuperscript{78} Article 8 (2) DPD.
3.3.4.1 Fair and lawful processing

The relationship between the controller and the data subject is governed by the fair processing principle.79 The DPD states in this regard that all processing must be fair and lawful.80 To begin with, fair and lawful processing presupposes that the processing is done in a transparent manner.81 The controller is obliged to inform the data subject before processing data relating to him/her, at least with regard to the identity of the controller, the purposes for which the data are intended and the existence of the right of access to and the right to rectify the data concerning him.82 Fair processing also entails that controllers are prepared to go beyond the minimum legal requirements of service to the data subject, if the data subject’s legitimate interests are at stake.83 Lastly, processing, in order to be lawful, must be carried out on one of the grounds listed in Article 7 DPD (cf. supra section 3.3.2).

3.3.4.2 Purpose limitation principle

The underlying aim of the purpose limitation principle is to respect the data subject’s reasonable expectations with regard to processing activities exercised on his or her personal data. Article 6 (1) b DPD states in this regard that personal data must be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.” The data controller has to explicitly specify - in advance - what he plans to do with the personal data. This also entails that every new purpose of processing, such as e.g. the disclosure of personal data to third parties, will require another legal basis.84 The compatibility between the purposes specified at collection and the way in which the data are further processed (re-use) will be assessed on a case-by-case basis.85

The Data Protection Directive further explicitly declares that the “further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.”86

3.3.4.3 Data minimisation

Pursuant to the Data Protection Directive, processing of personal data should be limited to data that are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.87 The controller should strictly limit data collection to the information that is directly relevant for the specific purposes of the processing.88 The controller further has to ensure at all times that the data are accurate and up-to-date.89 Another important requirement in this context is provided by article 6 (1) e DPD. This article obliges controllers to not keep the personal data for longer than necessary for the purposes for which it was gathered. The appropriate storage

79 Council of Europe, European Agency for Fundamental Rights, l.c., 73.
80 Article 6 (1) a DPD.
81 Council of Europe, European Agency for Fundamental Rights, l.c., 74.
82 Article 10 DPD.
83 Council of Europe, European Agency for Fundamental Rights, l.c., 75.
84 Council of Europe, European Agency for Fundamental Rights, l.c., 68.
85 Factors that are taken into account during the assessment of compatibility include: the relationship between the purposes for collection and the purposes of further processing, the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use, the nature of the data and the impact of the re-use on the data subjects, the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects. Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203, 2 April 2013, 23-27.
86 Article 6 (1) b DPD in fine.
87 Article 6 (1) c DPD.
88 Council of Europe, European Agency for Fundamental Rights, l.c., 70.
89 Article 6 (1) d DPD.
period will be determined on a case-by-case basis. Once the initial purpose for which the data was collected has been achieved, data controllers should either erase or anonymise the collected personal data.90

3.3.4.4 Data security and confidentiality

The DPD prescribes a duty of security. The aim of article 17 DPD is mainly to avoid data breaches. It obliges the controller to “implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.”

Providing appropriate access or using encryption techniques are examples of security measures. The necessary level of data security for each type of processing will be determined by the security features available in the market, the costs and the sensitivity of the data. There are also industrial, national and international standards that should be taken into account here. For example the European Network and Information Security Agency (ENISA) regularly circulates analyses of current security threats and provides advice on how to address them.91

Article 16 further provides a general duty of confidentiality on all persons, controllers or processors, with regard to the data they process. It states that “any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.” This provision concerns for example employees of controllers or processors. They have to ensure that the data remains confidential, by applying at least certain security measures before disclosing personal data.92

Further details on the specific data security and data breach notification aspects arising in the context of the CLARUS project will be discussed in chapter 4.

3.3.5 Data subject rights

Aside from the requirements for the processing of personal data, the data subject has a number of rights that he or she can exercise against the data controller. Furthermore, mechanisms are put in place to enable data subjects to enforce these rights.

3.3.5.1 Right to information

The first and arguably most important right for each data subject entails the right of him or her to receive certain information before the collection of personal data. Article 10 DPD provides that the controller should provide at least the following information:

“(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject such as
- the recipients or categories of recipients of the data,

90 Article 6 (1) e DPD.
91 Council of Europe, European Agency for Fundamental Rights, l.c., 90-91.
92 Ibid., 93.
whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him.”

The ideal way in which this information should be provided by the controller would be to address every individual data subject, orally or in writing. However, in practice this requirement is often fulfilled when the controller has appropriate information clauses published, such as a website privacy policy.93

3.3.5.2 Right of access

Every data subject has the right to receive more than the basic information of the controller about the data that is processed. Article 12 (a) refers to three types of information that the data subject has access to, without constraint at reasonable intervals and without excessive delay or expense:

“- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions.”94

Secondly, this right to access also entails a right of the data subject to rectify the data if it is inaccurate, or to erase or block the data if the processing does not comply with the Directive.95 There are certain limits to the data subject’s right of access. The obligation of controllers to grant the data subject’s access request may be restricted due to overriding legal interests of others.96

3.3.5.3 Right to object

The data subject further has the right to object to certain processing activities. This requirement needs to be evaluated on a case-by-case basis. The data subjects should prove that the processing of their data might affect them negatively and/or that the processing lacks a legitimate basis (anymore).97 The situations foreseen in the Directive are the right to object to automated individual decisions, to the data processing that leads to disproportionate results and to the use of their data for direct marketing purposes.

3.3.5.4 Right to legal relief

Finally, article 22 DPD provides every data subject with the possibility to seek a judicial remedy for any breach of the rights guaranteed to him or her by the national law applicable to the processing in question. Member States should further provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions is entitled to receive compensation from the controller for the damage suffered.98

93 Council of Europe, European Agency for Fundamental Rights, l.c., 98.
94 Article 12 (a) DPD.
95 Article 12 (b) DPD.
96 Article 13 DPD; Council of Europe, European Agency for Fundamental Rights, l.c., 106.
98 Article 23 DPD.
3.3.5.5 Data transfer

According to Article 1(2) DPD data transfer between Member States must not be restricted thus allowing for the free flow of data. In contrast data transfers to third countries are subject to specific restrictions. Article 25 provides that the Commission may ban data transfer to countries that fail to provide ‘an adequate level of protection’ of data privacy rights. Article 26 lists a number of derogations and provides that a transfer to a country that ‘does not ensure an adequate level of protection’ may occur if the controller enters a contractual arrangement that guarantees adequate safeguards for the protection of the fundamental rights and freedoms of the data subject.99 However, as noted by the Article 29 Working Party:

“cloud computing is most frequently based on a complete lack of any stable location of data within the cloud provider’s network. Data can be in one data centre at 2pm and on the other side of the world at 4pm. The cloud client is therefore rarely in a position to be able to know in real time where the data are located or stored or transferred. In this context, the traditional legal instruments providing a framework to regulate data transfers to non-EU third countries not providing adequate protection, have limitations.”

The draft regulation recognises the growing importance of international data transfers and reflects this new reality by abandoning the presumption that personal data cannot be transferred without an adequate level of protection. Instead, the Commission has opted to outline a number of requirements which must be satisfied before any such a transfer can occur.100 These modifications are provided in Articles 40-45 and include examples of the criteria that the commission would use in their assessment of the adequacy of the level of protection provided by the third country.

This is a very topical area, especially given the recent challenge to the legitimacy of such transfers to the US and the Safe Harbour agreement.101 In the context of CLARUS this has a particular significance in relation to the secure storage of cloud data. As per the Article 29 Working Party:

“the Safe Harbor principles by themselves may also not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the US, as may be required by national legislations based on the DPD. In terms of data security cloud computing raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures, which are not sufficiently addressed by the existing Safe Harbor principles on data security. Additional safeguards for data security may thus be deployed; such as by incorporating the expertise and resources of third parties that are capable of assessing the adequacy of cloud providers through different auditing, standardization and certification schemes. For these reasons it might be advisable to complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud.”102

This area has increased significance given the pending case before the Court of Justice and developments in this area should be watched closely in order to decipher any potential impact on the CLARUS project.

101 CJEU C-362/14 Reference for a preliminary ruling from High Court of Ireland (Ireland), 25 July 2014, Maximillian Schrems v Data Protection Commissioner.
3.4 E-Privacy Directive 2002/58/EC

The E-Privacy Directive\textsuperscript{103} (hereinafter ePD) was adopted in 2002 and later amended in 2009, with the aim of further particularising and complementing the provisions of the DPD.\textsuperscript{104} The ePD only applies to the processing of personal data in the electronic communication sector, or in other words the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.\textsuperscript{105} This means that all matters not under the scope of the ePD will be covered by the provisions of the Data Protection Directive. The ePD also provides that the provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services.\textsuperscript{106} These providers are obliged to protect both the privacy of natural users as well as legal person subscribers.\textsuperscript{107} The ePD excludes activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.\textsuperscript{108}

It is further noteworthy that certain provisions in the ePD are already considered general provisions. Therefore, the application of these provisions is not limited to electronic communication services. These general, key, provisions include article 5 (3) on cookies and article 13 on unsolicited communications.\textsuperscript{109}

3.4.1 Applicable provision analysis

3.4.1.1 Location data

Three types of data are mentioned in the ePD that can be generated during the course of a communication. In the context of CLARUS, it is interesting to first address location data. This category includes all data indicating the geographic position of the terminal equipment of a user\textsuperscript{110}, in particular information regarding the latitude, longitude or altitude of the terminal equipment; the direction of travel of the user; or the time the location information was recorded.\textsuperscript{111} According to article 9 (1) of the ePD, the provider can only process location data when they are anonymised or after obtaining consent of the user or subscriber, to the extent and for the duration necessary for the provision of a value added service. Prior to obtaining the consent of the users or subscribers, the provider must inform them of the type location data, the purposes, duration of the processing and whether the data will be transferred to any other third parties to provide the value added service. With regard to consent, the e-Privacy Directive requires a specific informed consent for each value added service requested. The provider must give the user or subscriber the possibility, using a simple means and free of charge, of temporarily refusing the

\textsuperscript{104} Article 1 (2) ePD; Council of Europe, European Agency for Fundamental Rights, l.c., 167.
\textsuperscript{105} Article 1 (1) ePD and Article 3 ePD.
\textsuperscript{106} Article 4 ePD.
\textsuperscript{107} Article 1 (2) ePD.
\textsuperscript{108} Article 1 (3) ePD.
\textsuperscript{110} Article 2 (c) ePD.
processing of such data for each connection to the network or for each transmission of a communication.\textsuperscript{112}

3.4.1.2 Content data

The second type of data generated during the course of a transmission is the actual content data. This data constitutes the content of the message and is logically strictly confidential. In particular, the Member States have to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned. However, technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality is still allowed.\textsuperscript{113}

3.4.1.3 Traffic data

Already mentioned supra, the third type of data mentioned in the ePD is traffic data, which comprises any data processed for the purpose of the conveyance of a communication on an electronic communications network.\textsuperscript{114} This traffic data enjoys the same level of confidentiality as content data, since it may consist of data referring to the routing, duration, time or volume of a communication\textsuperscript{115}, and thus contain personal information. Without the consent of the users, it is prohibited to listen, tap, store or in another way intercept or surveill their traffic data.\textsuperscript{116} The only exceptions to this rule are the use of traffic data for billing purposes and for technical storage which is necessary for the conveyance of a communication. Article 6 (1) states in the latter circumstance that the data must be erased or made anonymous when it is no longer needed for the purpose of the transmission. With regard to the consent requirement, article 5 (3) ePD more specifically requires the provider to obtain express consent of the user before installing cookies.

Next to the consent requirement, the provider will also have to ensure that traffic data is only processed for marketing purposes or for the provision of value added services. The provider can only process the data after informing the user/subscriber of the types of traffic data which are processed and the duration necessary for such services or marketing.\textsuperscript{117} Users or subscribers shall further be given the possibility to withdraw their consent for the processing of traffic data at any time.\textsuperscript{118} Lastly, processing of traffic data must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service. The processing must be restricted to what is necessary for the purposes of such activities.\textsuperscript{119}

3.4.1.4 Security of Processing

Article 4 ePD foresees the measures that providers must take into account to ensure a level of security during their processing activities. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security.

\textsuperscript{112} Article 9 (2) ePD.
\textsuperscript{113} Article 5 ePD.
\textsuperscript{114} Article 2 (b) ePD.
\textsuperscript{115} Recital 15 ePD.
\textsuperscript{116} Article 5 ePD.
\textsuperscript{117} Article 6 (4) ePD.
\textsuperscript{118} Article 6 (3) ePD.
\textsuperscript{119} Article 6 (5) ePD.
3.5 Proposed Data Protection Regulation

In January 2012, the European Commission released the proposal for a new legal framework for the protection of personal data in the EU, intended to replace the DPD. The Commission realised that the rapid pace of technological change and globalisation had profoundly transformed the way in which an ever-increasing volume of personal data is collected, accessed, used and transferred. They focused on reinforcing individuals’ rights, strengthening the EU internal market, ensuring a high level of data protection in all areas, ensuring proper enforcement of the rules and setting global data-protection standards. The Draft Regulation will, unlike the DPD which it replaces, be directly applicable in the Member States. It will further have a significant and wide-ranging impact on businesses, as it introduces new compliance obligations and promising significant sanctions in situations of non-compliance. Following this Draft, the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs (LIBE) released an adjusted compromise text, which the European Parliament approved in March 2014. These amendments are currently the basis for negotiations between the Commission, Parliament and the Council of Ministers. Delegations had received a revised version of the draft General Data Protection Regulation by the Council on 19 December 2014. This will be the basis for this section of the deliverable. Once the Regulation is agreed upon, the Draft prescribes that it will take two years before it becomes law. However, many organisations have already initiated preparations for these legislative changes.

3.5.1 Scope of the regulation

The material scope of the Proposed General Data Protection Regulation (hereinafter GDPR) covers the processing of personal data wholly or partly by automated means, and the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

The territorial scope of the GDPR is broader than the above discussed scope of the DPD. This Regulation shall apply to the processing of personal data in the Union. The GDPR however also covers the processing of personal data of data subjects residing in the Union by a controller not established in the Union. In this scenario, the processing activities have to relate to such data subjects in the European Union or the monitoring of their behaviour. Lastly, the Regulation applies to the

126 Article 2 (1) GDPR. This Regulation shall however not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security; (b) by the Union institutions, bodies, offices and agencies; (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity; (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Article 2 (2) GDPR).
processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.\(^{127}\) These last two scenarios entail that the processing of personal data of EU subjects will automatically fall under the scope of the GDPR, regardless of the foreign nature of the entity processing the data.

### 3.5.2 Key proposed changes

Article 4 of the GDPR includes certain new definitions that seem particularly interesting in the context of CLARUS. The most relevant updated and new definitions are:

```
(3b) ‘pseudonymisation’ means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution.

(8) ‘the data subject’s consent’ means any freely-given, specific, and informed indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

(9) ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(10) ‘genetic data’ means all personal data relating to the generic characteristics of an individual that have been inherited or acquired, resulting from an analysis of a biological sample from the individual in question;

(11) ‘biometric data’ means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data;

(12) ‘data concerning health’ means data related to the physical or mental health of an individual which reveal information about his or her health status.”
```

Recital 23 further discusses pseudonymisation:

```
[d]ata including pseudonymised data, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person (...)The application of pseudonymisation to data can reduce the risks for the data subjects concerned and help controllers and processors meet their data protection obligations. The explicit introduction of ‘pseudonymisation’ through the articles of this Regulation is thus not intended to preclude any other measures of data protection (...)National law may also provide for specific and suitable technical implementation measures for pseudonymisation and additional requirements for encryption.
```

Article 5 of the GDPR covers the principles related to the processing of personal data. The Article first of all provides clarification by expressly including the principles of transparency and data minimisation. Those principles are only implicitly recognised in the current DPD.\(^{128}\) Despite the fact that these principles have existed for 25 years, this proposal represents the first time they have been expressly stipulated in a legislative text.\(^{129}\)

Personal data must still be processed lawfully, fairly and in a transparent manner; collected for specified, explicit and legitimate purposes; adequate, relevant, and not excessive in relation to the purposes for

---

\(^{127}\) Article 3 GDPR.


\(^{129}\) L. Mitrou and M. Karyda, *EU’s Data Protection Reform and the right to be forgotten - A legal response to a technological challenge?*, 5th International Conference of Information Law and Ethics Corfu-Greece, June 2012, 1-23.
which they are processed; accurate and, where necessary, kept up to date; kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; processed in a manner that ensures appropriate security of the personal data.\footnote{Article 5 GDPR.}

Aside from the traditional data protection principles that were already included in the DPD, the GDPR introduces certain new principles and requirements that the data controller has to comply with in the context of processing activities. The key proposed changes will be discussed more in detail.

a. **Accountability and audit** - The principle of accountability in practice obliges the data controller to adopt internal policies and mechanisms that ensure compliance with the data protection rules. The controller must also be able to demonstrate this compliance with evidence. Furthermore, article 33 of the Regulation obliges data controllers to conduct a Data Protection Impact Assessment.

b. **Security and Notification** - Similarly as in the DPD, data controllers have a duty to implement appropriate technical and organisational measures to protect their processing activities. Additionally, the Regulation requires data controllers to develop or introduce these measures at the outset (privacy by design).\footnote{Article 23 GDPR.} This principle of ‘privacy by design’ will be discussed further on in this chapter. Article 31 of the new Regulation further includes an obligation to notify any breach of data without undue delay to the supervisory authority, where feasible within 72 hours after having become aware of it.

c. **Data subject’s rights** - The new Regulation provides more rights for data subjects than the current framework. With regard to the right to information, access, rectification and erasure, the data controller has a duty under the GDPR to implement transparent and easily accessible policies regarding the processing of data and the exercise of data subjects’ rights.\footnote{Article 11 GDPR.}

d. **Fines** - Sanctions can arise for the data controller or processor in case of non-compliance with the data protection rules. These administrative fines imposed shall in each individual case be effective, proportionate and dissuasive.\footnote{Article 79 (c) of the European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation, 12 March 2014, \url{http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN}.}

### 3.5.2.1 Privacy by Design

Due to the rapid developments and new possibilities of communication technology, both consumers and users encounter an increasing need to take into account privacy issues in the development stage. Particularly the choice of incorporating privacy into networked data systems and technologies as a default setting is gaining momentum.\footnote{A. Cavoukian, Privacy and Security by Design: A Convergence of Paradigms, available at \url{https://www.ipc.on.ca/images/resources/pbd-convergenceofparadigms.pdf}.} The aim of privacy by design is to protect privacy “by embedding it into the design specifications of information technologies, accountable business practices, and networked infrastructures, right from the outset”.\footnote{A. Cavoukian, Privacy by Design in Law, Policy and Practice; A White Paper for Regulators, Decision-makers and Policy-makers, available at \url{https://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf}.}

Privacy by Design encourages the idea of designing and implementing procedures and systems in accordance with privacy and data protection, already at their planning stage right until the deployment,

---

notably through the use of privacy-enhancing technologies.\textsuperscript{136} Certain elements of this theory were not entirely new. For example article 17 of the DPD already requires the data controller to implement ‘appropriate technical and organisational measures’.\textsuperscript{137} Since the provisions in the current framework in practice had not been sufficient in ensuring that privacy is embedded in ICT, the Article 29 Working Party therefore suggested that the new legal framework has to include a provision translating the currently punctual requirements into a broader and consistent principle of privacy by design.\textsuperscript{138} The Proposed GDPR of the European Commission took this opinion into account. According to Article 23 of the GDPR, having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.\textsuperscript{139}

The objectives of Privacy by Design consist of ensuring privacy and gaining increased control over one’s information. For organisations, it consists of gaining a sustainable competitive advantage.\textsuperscript{140} According to Cavoukian, these goals should be accomplished by taking into account the following 7 Foundational Principles\textsuperscript{141}:

1. **Proactive not Reactive, Preventive not Remedial**: The Privacy by Design approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2. **Privacy as the Default Setting**: We can all be certain of one thing – the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

3. **Privacy Embedded into Design**: Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. **Full Functionality (Positive-Sum not Zero-Sum)**: Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. **End-to-End Security (Lifecycle Protection)**: Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all


\textsuperscript{137} Recital 46 of the same Directive also demands such measures to be implemented from the design phase of the processing system on as well as at the time of the processing.


\textsuperscript{139} Article 30 of the GDPR on security of processing further highlights the developments in technology and solutions for privacy by design and data protection by default.

\textsuperscript{140} See: www.privacybydesign.ca.

\textsuperscript{141} Available at https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/.
data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.

6. **Visibility and Transparency:** Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. **Respect for User Privacy:** Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

### General objectives for Privacy by Design

The Article 29 Working Party on their part put forth seven general aspects / objectives one must take into account in the design stage of a processing system, its acquisition and the running of such a system:

1. **Data Minimisation:** data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all or as few personal data as possible.
2. **Controllability:** an IT system should provide the data subjects with effective means of control concerning their personal data. The possibilities regarding consent and objection should be supported by technological means.
3. **Transparency:** both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access / information should be enabled.
4. **User Friendly Systems:** privacy related functions and facilities should be user friendly, i.e. they should provide sufficient help and simple interfaces to be used also by less experienced users.
5. **Data Confidentiality:** it is necessary to design and secure IT systems in a way that only authorised entities have access to personal data.
6. **Data Quality:** data controllers have to support data quality by technical means. Relevant data should be accessible if needed for lawful purposes.
7. **Use Limitation:** IT systems which can be used for different purposes or are run in a multi-user environment (i.e. virtually connected systems, such as data warehouses, cloud computing, digital identifiers) have to guarantee that data and processes serving different tasks or purposes can be segregated from each other in a secure way.  

However, the practical application of these above objectives remains difficult to incorporate. With this in mind the focus should now turn to the means of implementation and as such design strategies.

### Privacy and data protection – design strategies

Hoepman further outlined 8 Privacy by Design strategies in his analysis of the application of the privacy by design principles. Both data oriented and process oriented strategies are represented in the following tables:

---


### Data Oriented Strategies

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Description</th>
<th>Design patterns/implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimise</td>
<td>Only the minimum amount of personal data should be collected.</td>
<td>For example “Select before you collect” and “anonymisation and use pseudonyms”.</td>
</tr>
<tr>
<td>Hide</td>
<td>Personal data and their interrelationships should be hidden from plain view thereby reducing the risk of abuse (an example of such an identifier would be an IP address).</td>
<td>For example the encryption of data, the use of mix networks to hide traffic patterns, the use of anonymisation or techniques to unlink the relationship between related events.</td>
</tr>
<tr>
<td>Separate</td>
<td>The processing of the personal data should be in a distributed fashion, this would prevent the completion of full profiles of individuals. Personal data should be processed in separate compartments; by separating the processing or storage of several sources of personal data that belong to the same person, complete profiles of one person cannot be made.</td>
<td>Currently no specific design patterns for this strategy are known.</td>
</tr>
<tr>
<td>Aggregate</td>
<td>The highest level of aggregation should be used including the least amount of detail as this will restrict the amount of personal data that remains.</td>
<td>Examples include: Dynamic location granularity, k-anonymity and other anonymization techniques.</td>
</tr>
</tbody>
</table>

Table 1: Data Oriented Strategies

The four data orientated strategies discussed above primarily address the principles of necessity and data minimisation.

### Process Oriented Strategies

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Description</th>
<th>Design patterns/implementation</th>
</tr>
</thead>
</table>

---

144 B. Jacobs, ‘Select before you collect, 2005, 54 Ars Aequi 1006.
146 G. Danezis et al., *l.c.*, 20.
147 Ibid.
149 G. Danezis et al., *l.c.*, 21.
### Privacy and data protection - design requirements

Having identified these general objectives and strategies certain requirements can be extrapolated. These could involve the following:

- Privacy should be proactive and not reactive and thus should be implemented as a default setting embedded into the design. This could involve the implementation of an automated anonymization/encryption process.
- The security of the personal data should be protected throughout the data lifecycle and this could involve encryption and also the coordination of Privacy Impact Assessments.
- Encryption should be employed throughout with the default state of data being unreadable if there is a data leak. This encryption should be applied automatically.
- Access to the personal data should be on a need-to-know basis only and should be restricted to specific employees. This could be achieved through authentication protocols with privacy features such as the Just Fast Keying protocol.\(^\text{151}\)
- The creation of measures (technological, policy and procedural) which bar the linking of personal data thereby respecting the data minimisation and purpose limitation principles.
- All personal data should be securely disposed of at the end in compliance with the limited retention of data principle. This should leave no trace of personal data in order for the process to be truly complete and compliant with the legal requirements relating to personal data retention and deletion.

---

\(^\text{150}\) In this context is interesting to look at proposed amendments Data Protection reform packages and in the draft NIS Directive (cf. infra section 4.3.2): where such an obligation is foreseen.

\(^\text{151}\) G. Daneis et al., l.c., 21.
From this analysis it is clear that there is a clear focus on the security of the data processing. Given that the CLARUS solution aims at its core to establish more secure storage of information and by extension personal data these requirements are satisfied by the very purpose of the processing to be implemented in the design of the CLARUS proxy.

However, it must be noted that although CLARUS aims to increase security of Cloud storage any potential personal data storage on the CLARUS proxy itself must also ensure the protection of the integrity of this data and thus compliance with the data protection provisions. With this in mind, although CLARUS may be classified generally as a privacy enhancing technology it should also ensure a privacy-by-design implementation. This notion is inextricably linked with the notion of security-by-design. There are several European instruments which promote the use of standards and/or specifications related to network and information security and promote stakeholder stimulation of industry-led security standards technical norms and security by design and privacy by design principles. It is with this in mind that our attention will now turn to a more detailed examination of security related legal provisions.

3.6 Conclusion

As noted from the above discussion, the data protection and privacy framework outlines specific requirements that have relevance for CLARUS. The project’s focus on the security of cloud stored data explicitly indicates a reliance on the safeguards to be implemented regarding the protection of personal data. However, for a more comprehensive overview, a more detailed examination of the security specific considerations is needed.

152 See: The NIS Directive, the Cybersecurity Strategy of the European Union, the Recommendation 2012/148/EU.
4 Security, breach notification and contractual mitigation of liability

The purpose of this chapter is to analyse the key legal issues regarding security in relation to the CLARUS project. The analysis aims to build on the analysis provided in relation to security aspects as mentioned in Chapters 2 and 3 and provide a detailed overview of the security related requirements.

4.1 Protecting integrity and authenticity of confidential data and guaranteeing access

Given the growing number of cyber-attacks, guaranteeing the integrity of security systems is becoming increasingly challenging. Indeed, as is observed by Cronin, “the only way to protect a computer from the Internet threats is to unplug it, both from a telecommunication connection and from the wall.”\(^{(153)}\) It is with this backdrop that CLARUS aims at providing its solution. Nevertheless, for a complete analysis one must be aware of the other security related provisions. As was made clear in the above analysis both Directives 95/46/EC and 2002/58/EC provide for specific provisions requiring the secure processing of personal data. However, in relation to the CLARUS use cases it is also apparent from the analysis provided in Chapter 2 that specific restrictions related to the dissemination of the relevant geo-spatial data to the public may exist.

Accordingly, this requires specific access controls and security mechanisms in order to prevent unauthorised access and/or alteration of a data set. Indeed the protection of the integrity, authenticity and confidentiality of the stored information are key elements of the security standards. In addition, a significant element of security not only relates to the data availability and the protection of data against accidental or wilful destruction or loss.\(^{(154)}\) Such actions may have a crippling effect on cloud users and as such security protocols and mechanisms need to be established in order to counteract external events affecting data availability. In the context of the CLARUS project such protections are the very purpose of the project as it aims to reduce the risks associated with cloud storage. As the scope of the use cases deal specifically with personal data one must consider the specific concerns imposed in relation to public communication networks and the proposed changes in the General Data Protection Regulation.

4.2 Encryption, anonymisation - holding the keys to personal data access.

As is clear from the purposes of the project the CLARUS solution focuses on the secure storage of data through the encryption and anonymisation of the stored data. From a privacy and data protection perspective this has potentially relevant consequences as the stored data may not be in an intelligible form thus potentially having consequences for the classification of the cloud service provider as a data controller (cf. supra section 3.3.1.2). For example, the lack of a possibility to identify is currently hotly debated in relation to dynamic IP addresses. This issue is currently pending before the Court of Justice of European Union. On the 28th of October 2014 the German Federal Court (Bundesgerichtshof) referred a question on the status of dynamic IP addresses to CJEU.\(^{(155)}\) Specifically, the referring court is seeking to clarify whether a dynamic IP address constitutes personal data if the IP address itself is stored by an


\(^{(155)}\) See: http://www.google.com/url?q=http://juris.bundesgerichtshof.de%2Fcgi-bin%2Ffrechtsprechung%2Ddocument.py%3FGericht%3Dbgbh%26Art%3Dpdm%26Datum%3D2014%26Sort%3D3%26nr%3D69184%26pos%3D0%26anz%3D152&aFAIL%3DA%26sntz%3D1%uASr%3DAFQcJcNE7JkxgMXi55SN5nzkUXWothT7Lpq
Internet service provider (ISP) while the information required to identify the user based on this IP address is held by a third party.\textsuperscript{156} There are clearly dividing opinions in the Member States. However, in its opinion on the concept of personal data the Working Party has stated that as static and dynamic IP addresses are not in practice easily distinguishable all IP addresses should consequently be treated as personal data.\textsuperscript{157} This opinion in essence fails to truly categorise dynamic IP addresses as personal data but instead recommends a \textit{de facto} status based on the inability of services providers to distinguish between the types of IP addresses.\textsuperscript{158} This will be an issue that the Court will be required to consider carefully.

Developments in this regard should be closely followed. However, despite these issues in relation to the data that will be stored, the format it will be stored in and the consequences \textit{vis-a-vis} its legal status, it should also be noted that other personal data may be gathered by the cloud service provider in order to verify authentication and access controls. Accordingly this still remains clearly relevant as they will be responsible for the processing of this personal data. With this in mind it is necessary to analyse security specific elements such as notification requirements for personal data breaches.

### 4.3 Breach notification obligations

Currently in the context of data protection and privacy, notification requirements are restricted in application to the communications sector with both the e-Privacy Directive and the recent Data Breach Notification Regulation\textsuperscript{159} providing such obligations and the provision of a communication network or service to the public.\textsuperscript{160} Specifically in relation to CLARUS it must be noted that CSPs do offer such a public service. Therefore, the CLARUS solution may also be classified as such if personal data is stored and if the service is generally accessible to the public.

Although Directive 95/46/EC does not provide a general personal data breach notification requirement this does not prevent Member States from implementing such a general obligation. For example in Germany a breach notification duty was added in section 42a of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG).\textsuperscript{161} This applies in relation to sensitive personal data and personal data related to:

- secrecy;
- criminal and or administrative offices;
- bank or credit card accounts; and
- certain telecommunications and online data.


\textsuperscript{161} Bundesdatenschutzgesetz [Federal Data Protection Act], Dec. 20, 1990, BGBl. I at 2954, as amended.
This contrasts sharply with the legislation in other Member States and thus there is a degree of disparity in relation to this issue across the EU. In Ireland and the UK the Data Protection Authorities have issued Codes of Conduct on the requirement to report data breaches generally. However, this is soft law and currently Germany is the only Member State that extends this requirement beyond the telecommunications sector in hard law. However, it should be noted that there are some proposed changes in this regard which need to be considered in the proposed GDPR. The analysis will now examine the requirements as provided in Directive 2002/58/EC and Regulation 611/2013 before then examining the proposed modifications of Directive 95/46/EC.

4.3.1 Electronic communication networks and services

Article 2(i) of Directive 2002/58/EC (as amended) provides that a “personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.” As previously indicated this Directive requires personal data breaches to be notified to the competent national authority. This requirement is specified in detail in Article 4. Furthermore, Article 4(3) specifies that when such a breach is “likely to adversely affect the personal data or privacy of a subscriber or individual” the service provider is required to notify this person of the breach without “undue delay”. This requirement is independent of the obligation to notify the relevant national authority. According to Article 2 Regulation 611/2013, “[t]he provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible.” Following from this initial notification the service provider is required to make “a second notification to the competent national authority as soon as possible, and at the latest within three days following the initial notification.”162 Regulation 611/2013 provides detailed information on the type of information which must be reported in Section 1 of Annex I to the Regulation. However, as noted by the Article 29 Working Party opinion on the personal data breach notification requirement, the framework provides:

“[A]n exemption on the notification requirement to data subjects if the data have been rendered unintelligible. If the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures to render the data unintelligible to any person who is not authorised to access it and if those measures were applied to the data concerned by the security breach, then notification of a personal data breach to a data subject shall not be required.”

This is specified more particularly in Article 4(3) Directive 2002/58/EC and Article 4(1) Regulation 611/2013. In order for data to be considered unintelligible it must satisfy one of two conditions as provided under the Regulation namely:

“a) it has been securely encrypted with a standardised algorithm, the key used to decrypt the data has not been compromised in any security breach, and the key used to decrypt the data has been generated so that it cannot be ascertained by available technological means by any person who is not authorised to access the key; or

(b) it has been replaced by its hashed value calculated with a standardised cryptographic keyed hash function, the key used to hash the data has not been compromised in any security breach, and the key used to hash the data has been generated in a way that it

---

162 Article 2(3) Regulation 611/2013
cannot be ascertained by available technological means by any person who is not authorised to access the key.”

This derogation reflects the reality that such privacy measures may mitigate the residual privacy risk associated with the breach thereby reducing the privacy risk to a negligible level and thus protecting the data subject. However, and as noted by the Article 29 Working Party “even when data is encrypted, a loss or alteration can have negative effects for data subjects when the data controller has no adequate backups. In this case notification to data subjects should still be required even with encryption protection measures in place.” In the context of CLARUS this has a clear potential impact upon the providers of a cloud service.

### 4.3.2 Proposed breach notification obligations

The draft GDPR proposes the introduction of an obligation to notify personal breaches in Articles 31 and 32. This establishes the requirement that personal data breaches must be notified to the relevant parties “without undue delay”. Given the increased frequency of data breaches this is one of the least controversial reforms in the proposal. Moreover, from Article 30(3) of the proposed GDPR, the security of personal data appears to have been aligned with the concepts of privacy by design and by default. This move towards the implementation of a notification requirement is further reflected in the proposed Police and Criminal Justice Data Protection Directive and in the area of network and information security in the form of the proposed NIS Directive. However, it should be noted that CLARUS remains outside the scope of both these proposed Directives.

### 4.4 Cloud service provider liability

In the following section, the cloud service provider liability will be analysed. This analysis is based on the liability on civil (contractual) and tort law. This proceeds the detailed overview of the requirements related to electronic commerce law and more specifically the liability of intermediaries. It must be noted that this area is dictated by the principle of subsidiarity and thus in order to have a detailed overview of requirements one must refer to national law. However, some general guidance specific to cloud services is outlined below. Generally, a liability claim will need to fulfil four elements in order to be admissible:

- An illegal act of the CSP
- A quantifiable damage;
- Causality between the act and the damage occurred;
- Fault (gross/light negligence) by the CSP.

There will however be liability limitations/exemptions for the CSP in some circumstances.

---

163 Article 4(2) Regulation 611/2013.
166 M. Hildebrandt and L. Tielemans, Data protection by design and technology neutral law, Computer law and Security Review, 2013, 29, 509.
169 The most recent version of the NIS Directive restricts its application to Critical Infrastructures
4.4.1 Contractual mitigation of liability
First of all, contractual clauses can limit or exclude liability for the CSP or contain an indemnification of a party against losses. Via contract, the parties will often regulate server availability, consequences of losses after periods of server downtime, disaster recovery and back-up strategy. As noted in Chapter 2 cloud service providers will often want to use data to improve their services, the security requirements, the audit rights, the incident response, the keeping of data confidential and the availability of services in case of fast user growth. Traditionally the cloud service provider will have a much higher bargaining power than the cloud user, who will have to accept a standard low protection or lose the possibility to use the service. Nevertheless, the CSP could be subject to direct liability once the user experiences losses of the data hosted on the cloud, or where the data has been compromised. Standard cloud contracts will often contain disclaimers against indirect liability of the CSP, as this indirect liability can have a potentially very large scope. Most CSPs therefore explicitly exclude liability for the direct loss resulting from the deletion of customer data, since this loss can be very high for a business. Most CSPs further set maximum liability that is often a multiple of the amount paid in service fees. Many cloud contracts further contain licensing provisions that allow the CSP to process any data stored on its servers, predominantly for targeting purposes.

4.4.2 Negligence - tort liability
When there was no breach of contract, a liability claim under the tort of negligence will serve as an alternative. In this case, the complainant will have to establish a duty of care of the CSP and prove a breach that resulted in causal damages. Since a specific duty of care for a cloud provider has not yet been established in case law, one must, in case of a breach, consider whether an ordinary, prudent and reasonable cloud provider would have acted differently in preventing the harm.

4.5 Conclusion
The examination of the legal and ethical obligations related to the security specific provisions impacting upon the CLARUS solution has revealed certain key requirements. It is clear that CSPs aim to mitigate the responsibilities through contractual mechanisms. Such considerations are relevant for CLARUS. Nevertheless, for a more detailed overview of the requirements relevant for the content stored on the cloud, the analysis will now turn to an examination of internet intermediary liability under the E-Commerce framework. Following this analysis, public sector access to this cloud data will be examined in detail.

---

171 Ibid.
172 Ibid, 4.
174 Ibid.
175 See e.g. Facebook Privacy Terms, available at https://www.facebook.com/policy.php.
176 R.H. Weber and D.N. Staiger, l.c., 7.
5 Liability of intermediaries

Internet intermediaries are actors, who are placed between two (or more) different parties to intermediate between them. They serve as enablers of the communications between these parties. The Organisation for Economic Co-operation and Development (OECD) envisions the role of Internet intermediaries as “bring[ing] together or facilitat[ing] transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.” Examples of intermediaries, are internet service providers (ISPs), hosting providers, search engines, e-commerce intermediaries, Internet payment systems and participative Web platforms.

Figure 1: Stylised representation of Internet intermediaries’ roles. Source: OECD, The Economic and Social Role of Internet Intermediaries

This chapter of the deliverable provides a coherent overview of the legal framework governing the liability of the Internet intermediaries in the European Union. More in detail, the present deliverable provides an analysis of the E-Commerce Directive 2000/31/EC and its special regime for intermediaries. The relevant sections of the Directive for CLARUS will be analysed and the conditions with which different intermediaries need to be in compliance will be defined. As Member State legislation stems from the E-Commerce Directive, the chapter will focus on the EU legal framework.

5.1 EU regime on liability of intermediaries

Directive 2000/31/EC, commonly referred to as the E-Commerce Directive (ECD), regulates the liability of Internet intermediaries in the European Union. The Directive aims to establish a clear and general framework to cover certain legal aspects of electronic commerce in the internal market. It applies to ‘information society services’, which are defined as “any...
service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services” (Article 2(a) ECD).\textsuperscript{181}

The element of remuneration in the definition refers mainly to the existence of an economic activity or an activity for which an economic consideration is given in return.\textsuperscript{182} The element ‘at a distance’ implies that the parties cannot be simultaneously physically present in the same place.\textsuperscript{183} ‘By electronic means’ refers to every service that is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and the storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means.\textsuperscript{184} ‘At the individual request of a recipient of services” simply means that the service is provided through the transmission of data on individual request.\textsuperscript{185} Examples of the services falling under this broad definition may include (in so far as they represent an economic activity): online contracting, services providing transmission of information via communication networks, services providing access to a communication network, hosting of information, as well as services that do not give rise to on-line contracting, e.g. those offering online information or commercial communications or those providing tools that allow for search, access and retrieval of data.\textsuperscript{186} Article 1 ECD further excludes application of the Directive for certain services and activities such as questions covered by the Data Protection Directive.\textsuperscript{187}

5.1.1 Liability exemptions for intermediaries

The E-Commerce Directive provides liability exemptions for intermediary service providers for certain types of intermediary services in its Section 4. These exemptions exist for actions that could be considered as ‘mere conduit’ (article 12), ‘caching’ (article 13) or ‘hosting’ (article 14). These exemptions cover various types of illegal content (infringements on copyright law, defamation law, unfair commercial practices, etc.) and different kinds of liability (criminal, civil, direct, indirect).\textsuperscript{188} Before analysing the specific exemptions, it needs to be highlighted that the intermediary is not per se liable if the conditions for being exempt are not met. The intermediary merely stops falling under the immunity provided by the Directive.\textsuperscript{189}

5.1.1.1 Mere conduit

Article 12 provides for the liability exemption for providers of ‘mere conduit’ services which are defined as:

\textsuperscript{181} This provision refers back the definition in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC.
\textsuperscript{184} See art. 1, 2 of Directive 98/48/EC.
\textsuperscript{185} Art. 1, 2 of Directive 98/48/EC.
\textsuperscript{186} For more examples, see Recital (18) of Directive 2000/31/EC.
\textsuperscript{187} Article 1 (5) b ECD.
“- those services which consist of the transmission in a communication network of information provided by a recipient of the service (‘transmission services’); and
- those services which consist of the provision of access to a communication network (‘access services’).

Article 12 considers the service provider not liable for the information transmitted, on condition that the provider:
(a) does not initiate the transmission (of data);
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.”

Recital (42) further emphasises that the exemptions from liability only cover cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network. The activity covered by this exemption is of a mere technical, automatic and passive nature. In order to fall under the mere conduit regime, the information society service provider cannot have knowledge of nor control over the information which is transmitted or stored.

Lodder compares the services described in article 12 to postal services, as the providers of these services are also not held liable for possible illegal content in the letters. The acts of transmission and provision of access include the automatic, intermediate and transient storage of the information transmitted as long as this takes place for the sole purpose of carrying out the transmission in the communication network, and only if the information is not stored for any period longer than is reasonably necessary for the transmission (Article 12(2)).

Even when the conditions of article 12 are met, the possibility remains for a court or administrative authority to require the service provider to terminate or prevent an infringement, if the legal system of the Member State provides for this. In practice only a limited group of service providers, such as telecommunications operators and ISPs, will benefit from the ‘mere conduit’ exemption. Cloud service providers generally do not fall within this exemption.

---

190 This requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission (recital 43).
191 A literal reading of Recital (42) shows that it aims to address all of the exemptions of the Directive. However, one could argue that the scope of this part of the recital should be limited to the transmission and access services identified in articles 12 and 13. However, the exemption for hosting enshrined in art. 14 does not limit its scope to either transmission or access services. See also E. Montéro, Les responsabilités liées au web 2.0, Revue du Droit des Technologies de l’Information 2008, n° 32, p. 367. The ECJ has however disagreed with this viewpoint. It held recital (42) equally applicable to hosting services: see CJEU, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.), paragraphs 113-114.
193 Article 12 (3) ECD.
194 Certain Member States have however broadened the scope of their national legal framework to cover services provided by other intermediaries such as for example search engines: T. Verbiest et al., Study on the Liability of Internet Intermediaries, commissioned by the European Commission, 12 November 2007, p.4, 19, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.
5.1.1.2 Caching

The second liability exemption provided by the Directive relates to the ‘caching’ of information. The provision mainly targets providers of ‘proxy-servers’. Article 13 defines caching as ‘the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their request’. This exemption only applies when the intermediary provides information society services that consist of the transmission in a communication network of information provided by a recipient of the service (‘transmission services’). Recital (43) applies to both caching and ‘mere conduit’, since both these exemptions are limited to manipulations of a technical nature, that do not alter the integrity of the information contained in the transmissions. The exemption for caching services however only applies to transmission services (whereas the ‘mere conduit’ exemption prescribed in article 12.2 formally extends to access services).

The biggest difference between article 12.2 and 13.1 appears to relate to the purpose of the storage. Whereas article 12.2 aims to exempt transient storage which takes place for the “sole purpose of carrying out the transmission” caching under article 13.1 is performed “for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their request”. The following five conditions must further be met in order to benefit from the caching exemption:

- the (service) provider does not modify the information;
- the provider complies with conditions on access to the information;
- the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
- the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
- the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Just as in article 12.3, the caching exemption does not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement (article 13.2).

5.1.1.3 Hosting

Article 14 ECD covers the third liability exemption for Internet intermediaries. The article provides that where an information society service consists of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

---


197 The articles should be interpreted as only prescribing information society services which qualify as transmission services to benefit from art. 12.3, whereas both transmission services and access services are able to avail themselves of art. 12.2.

198 Article 13.1 ECD.
“- the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- the provider, upon obtaining such knowledge or awareness, immediately removes or disables access to the information.”

The typical service falling under this provision is a webhosting service that provides online space to its users, to upload content to be published on a website (e.g. YouTube).\textsuperscript{199} The storage by these ‘hosting’ service providers differs from ‘mere conduit’ and ‘caching’ transient storages.\textsuperscript{200} Hosting service providers do not store information merely ‘incidental’ when providing their transmission or access services.\textsuperscript{201} These hosting providers can further store the information for a prolonged period of time. Moreover, the storage can even be the primary object of the service.\textsuperscript{202}

The CJEU has clarified that the exemption only applies to providers that conduct their services in a neutral manner. The Court defined this neutral conduct as ‘technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores.’\textsuperscript{203} With regard to the interpretation of ‘actual knowledge’ in article 14.1a the CJEU stated in \textit{L’Oréal v. Ebay}\textsuperscript{204} that a service provider will only be exempt from any liability for unlawful data that it has stored on condition that it did not have “actual knowledge of illegal activity or information”.\textsuperscript{205} With regard to claims for damages, the service provider has to prove that it was not “aware of facts or circumstances from which the illegal activity or information is apparent” or that, having obtained such knowledge or awareness, it has acted expeditiously to remove, or disable access to, the information.\textsuperscript{206} The provider will be denied the exemption, when it should have been aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question.\textsuperscript{207} The threshold that the CJEU prescribes in this case is quite high, since any diligent economic operator who comes across the material has to identify it as being illegal.\textsuperscript{208}

Recital (46) further stipulates that “the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level”. These procedures for service providers are however not further regulated in the Directive, nor are there any other details or safeguards to ensure proportionality or due process of the removal or blocking.\textsuperscript{209} The analysis of the reliability of the notices of illegality has therefore proven to be difficult for the providers.\textsuperscript{210} Article 14.3 does provide the possibility for every Member State to establish “procedures governing the removal or disabling of access to information”. However, while some of the Member States

\textsuperscript{199} P. Van Eecke P. and M. Truyens, \textit{l.c.}, 9.
\textsuperscript{200} A. Kuczerawy and J. Ausloos, \textit{l.c.}, 6.
\textsuperscript{201} I. Walden in Bullesbach A., Poulet Y., Prins C. (eds.), \textit{l.c.}, p. 253.
\textsuperscript{202} Montéro therefore states that this exemption may in principle benefit any type of service provider who stores content at the request of the recipient (see Montéro, E., \textit{l.c.}, 369-373).
\textsuperscript{203} CJEU, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.), paragraphs 113-114.
\textsuperscript{204} European Court of Justice (Grand Chamber), C-324/09, 12 July 2011, (L’Oréal SA and others).
\textsuperscript{205} Paragraph 119.
\textsuperscript{206} Paragraph 119.
\textsuperscript{207} Paragraph 120.
\textsuperscript{209} A. Kuczerawy and J. Ausloos, \textit{l.c.}, 8.
have provided a more detailed regulation for the ‘hosting’ exemption by introducing formal Notice-and-Take Down procedures, many still leave this possibility enshrined in the Directive unattended.\textsuperscript{211}

A hosting service provider further cannot benefit from the exemption of article 14 when the recipient of the service is acting under the authority or the control of the provider.\textsuperscript{212} This situation arises for example when the service recipient is an employee of the service provider.\textsuperscript{213} Article 14 further also foresees the possibility for a national court or administrative authority to introduce prohibitory injunctions as the articles on mere conduit and caching.\textsuperscript{214}

5.1.1.4 No general obligation to monitor

Article 15 ECD states that Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor to actively seek facts or circumstances indicating illegal activity. Member States are prevented from imposing a monitoring obligation on service providers with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case nor does it affect orders by national authorities in accordance with national legislation.\textsuperscript{215} Obliging service providers to conduct general monitoring of content means that they would no longer act passive and neutral. Furthermore, general monitoring could even lead to censorship and have a consequential deterrent effect on the freedom of expression.\textsuperscript{216}

The Directive further does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.\textsuperscript{217} The duties of care are never defined in the Directive. This inadvertently blurs the difference between these duties and general monitoring. Recital 48 and article 15 can therefore be regarded as quite contradictory.\textsuperscript{218} It is further necessary to emphasise that the prohibition of general monitoring schemes according to article 15 only applies to service providers that provide ‘mere conduit’, ‘caching’ or ‘hosting’ services. Once certain service providers fall outside the scope of these regimes, Member States theoretically could try to impose general monitoring obligations on them.\textsuperscript{219} This has so far not been attempted in any of the Member States.

Finally, Member States have the possibility to impose two additional obligations upon information society services providers. First of all, they may oblige the providers promptly to inform the competent public authorities of alleged illegal activities by recipients. Secondly, the Member States may impose an obligation upon these providers to communicate to the competent authorities, at their request, the identity of recipients with whom they have storage agreements.\textsuperscript{220}

\textsuperscript{212} Article 14 (2) ECD.
\textsuperscript{213} A. Lodder, l.c., 89.
\textsuperscript{214} Article 14 (3) ECD.
\textsuperscript{215} Recital 47 ECD.
\textsuperscript{216} OECD, l.c., 36.
\textsuperscript{217} Recital 48. See also Court of Justice of the European Union, C-70/10, 24 November 2011 (Scarlet v. SABAM), and Court of Justice of the European Union, C-360/10, 16 February 2012 (SABAM v. Netlog).
\textsuperscript{218} R. J. Barceló and K. Koelman, l.c., p. 232.
\textsuperscript{220} Article 15 (2) ECD.
5.2 Applicability of the hosting exemption on a Cloud Service Provider

At this point of the deliverable, it is interesting to analyse whether CSPs could be liable for the actions of their users. The services offered by a CSP are generally not considered to be hosting activities. Some authors nevertheless consider that the hosting category is the most appropriate regime to apply in the context of cloud computing services, as Article 14 ECD is the most inclusive of the three exemptions.\textsuperscript{221} Even though the data storage and collection obligations of a CSP are not comparable to the obligations of a host provider facilitating Internet access to users\textsuperscript{222}, the services of the CSP seem to fall under the definition of ‘service’ under the Directive 98/48/EC.\textsuperscript{223} Cloud computing services are (often) remunerated services provided at a distance via electronic means on request of the recipient of such a service.

We can therefore assume that a CSP could be exempt from liability when it was not aware of illegal data being stored on its hardware.\textsuperscript{224} This exemption however does not cover situations in which the CSP only temporarily transports data through its RAM and automatically deletes this data from the temporary server memory once the intention to store it disappears.\textsuperscript{225}

As stated above, Article 14 (1) (a) ECD further states that a host provider can still be liable in case of negligence, i.e. when the provider has actual knowledge of illegal activity or information and is aware of facts or circumstances from which the illegal activity or information is apparent. In this regard, most cloud storage providers (such as e.g. Dropbox\textsuperscript{226}) include a contractual clause that provides them with the right to review the data stored by their users and to cancel the contract once the data breaches the company policy (e.g. includes obscene or other illegal content).\textsuperscript{227} In the context of CLARUS, given that the data will be encrypted, such action may be futile.

Finally, there are new types of cloud computing such as e.g. cloud hosting that has merged cloud computing and hosting services. The liability exemptions in the ECD are not equipped to cover these new types of technologies. Therefore, the CLARUS project will follow the ongoing review of the ECD and the developments with regard to the 2010 Notice-and-Action initiative of the European Commission.\textsuperscript{228}

5.3 Conclusion

From the overview of the specific provisions contained in the ECD, the requirements refer to obligations on the CSP side. As a result, for the purposes of CLARUS, the direct legal impact of these provisions is somewhat negligible. However, to ensure an effective implementation of the CLARUS solution, such an analysis is necessary in order for all parties to understand the detailed legal requirements relevant to cloud storage.

\textsuperscript{221} J.P. Sluijs, P. Larouche and W. Sauter, Cloud Computing in the EU Policy Sphere, JIPITEC 2012/1, 26.
\textsuperscript{222} R.H. Weber and D.N. Staiger, l.c., 3.
\textsuperscript{223} Article 1 (a) Directive 98/48/EC.
\textsuperscript{224} R.H. Weber and D.N. Staiger, l.c., 3.
\textsuperscript{225} Ibid.
\textsuperscript{226} Dropbox, Terms and Privacy Policy, www.dropbox.com/privacy#security.
\textsuperscript{227} R.H. Weber and D.N. Staiger, l.c., 3.
6 Public sector access to cloud data

This Chapter focuses on the access to cloud data by the public sector. It should be noted that in this regard such access relates to that sought by law enforcement agencies during the course of an investigation. This examination is key for an effective overview of the legal obligations given CLARUS’ aims. However, before beginning this analysis it is important to note the seminal decision\textsuperscript{229} which struck down the Data Retention Directive\textsuperscript{230} and found it to be invalid. As a consequence of this judgment, national implementations of this directive have unclear foundations with certain Member States taking action and declaring them invalid, and others such as the UK implementing emergency measures providing for their continued application. However, for the purposes of this analysis it remains outside the scope, as it is clearly been found in contradiction with EU law.

6.1 Cloud challenges and forensic investigations

The migration of data to the cloud brings the issue of unauthorised access to the fore. As described in the analysis provided thus far, the purpose of CLARUS is to increase security mechanisms in order to mitigate the effects of an attack and potential breaches. However, public law enforcement agencies may require access to data held in the cloud for the purposes of forensic investigations.

This brings with it two strands of problems. First, given the concerns regarding increasing surveillance many users wish to be ensured the integrity and confidentiality of their information. Second, cloud storage brings with a series of challenges which may render such investigations much more difficult. These problems are inextricably linked. A key issue in relation to this topic resides in the fact that this is an area which is dominated by national law. As such a large degree of disparity exists and given the jurisdictional flexibility of cloud services clear issues can arise in relation to common standards and measures regarding access of data for law enforcement agencies. However, before delving into the specifics it is significant to note that as per Walden cloud computing presents forensic challenges in four key areas, namely: the multiplicity of the data, that this data may involve distributed storage, that it may be protected (e.g. through encryption and authorities may only be able to get unintelligible data) and finally that it may be difficult to establish the link between the evidential data and the identity of a real world person.\textsuperscript{231} These concerns have a clear impact on CLARUS, as the project focuses on the secure encrypted storage of data, thereby rendering law enforcement agency access more troublesome.

Law enforcement agency access to data and the respective authorisation procedures can vary significantly across jurisdictions with differing oversight mechanisms. However, it should be noted that such agencies will generally be afforded express powers by Statute to operate and gain access under certain circumstances and particular controls. For many countries this involves the exercising of some form of warrant dependant on \textit{inter alia} the type of information to be accessed and the urgency of the matter (for example if it is a matter for national security). However as noted by Walden:

\textsuperscript{229} CJEU, Joined cases C-293/12 and C-594/12, \textit{Digital Rights Ireland and Seitlinger and others}, 8 April 2014.
“different procedures, safeguards and oversight mechanisms can generate uncertainty and
distrust about the sufficiency of protections that foreign regimes offer against abusive
deployment and infringements of individual rights.”

Indeed although these mechanisms have in built oversight mechanisms particularly in relation to the
administrative requirements associated with obtaining of the authorisation there remain certain
reservations in relation to the adequacy of these protections.

### 6.2 Convention on Cybercrime

At an international level there has been some attempt at harmonisation in the form of the Convention on
Cybercrime. However, despite the fact that this has been signed by 53 States 8 have failed to ratify
including Ireland, Greece and Sweden. Article 14(1) of the Convention states that “Each Party shall
adopt such legislative and other measures as may be necessary to establish the powers and procedures
provided for in this section for the purpose of specific criminal investigations or proceedings.” Indicative
of the discussion provided above Article 15 of the Convention outlines the conditions and safeguards
relevant for the exercising of these powers and procedures. In relation to access, the powers conferred
upon law enforcement agencies can be divided into those exercisable against the cloud user and those
against service providers.

Service providers are defined in Article 1(c) as:

“service provider’ means:

i any public or private entity that provides to users of its service the ability to
communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such
communication service or users of such service.”

For instance title 2 of the Convention regarding the expedited preservation of stored computer data and
more particularly Article 16 (expedited preservation of stored computer data) and Article 17 (Expedited
preservation and partial disclosure of traffic data), although potentially applicable to any persons is more
likely to be directed towards service providers. The precise requirements in relation to this preservation
requirement are unclear.

However, it must be understood that these provisions are separate from that of access with the
Convention specifically classifying two distinct types of production orders. As per Article 18(1):

“Each Party shall adopt such legislative and other measures as may be necessary to
empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person’s possession
or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber
information relating to such services in the territory of the Party to submit subscriber
information relating to such services in that service provider’s possession or control.”

In relation to the second of these “subscriber information” means:

“any information contained in the form of computer data or any other form that is held by
a service provider, relating to subscribers of its services other than traffic or content data
and by which can be established:

---

233 Convention on Cybercrime CET No.: 185 accessed on 21/01/2015 at: conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.
a. the type of communication service used, the technical provisions taken thereto and the period of service;

b. the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.”

As such it is clear from the analysis that these production orders are directed towards service providers.

Regarding cloud user, a search and seizure order as provided under Article 19 is the much more likely mechanism. From Article 19 (1):

“Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a. a computer system or part of it and computer data stored therein; and

b. a computer-data storage medium in which computer data may be stored in its territory.”

However, it should be acknowledged that this may also indirectly have an effect on the service provider. Indeed Article 19(2) stipulates that the initial search may be extended to other computer systems connected to the users where the other system is within the territory and is “lawfully accessible from or available to the initial system.”

The final article to be considered in relation to the Cybercrime Convention is Article 32 which deals with the trans-border access to stored computer data. This provision states that:

“A Party may, without the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.”

As noted by Walden, this does not preclude the creation of the measures related to transboundary access but rather represents a position that is acceptable to all parties.235 Aside from this direct transboundary access issue, Articles 25 and 26 of the Convention also stipulate provisions related to mutual assistance and spontaneous (or proactive) information sharing respectively.

Despite severe criticism,236 the Convention still holds significance given the global nature of cybercrime and access more narrowly.237 Without the adoption of these international mechanisms States “can only combat the more complex and generally international computer crime within the boundaries of limited domestic laws.”238 This also affects any potential prosecutions as even countries; “with extraterritorial jurisdictions are subservient to the procedures listed in designated extradition laws of one another, in the absence of which there may be ad hoc extradition agreements between countries.”239 However, Fahey

---

has observed that the relevance of the Convention may be waning given the change in the EU’s competence in this area. This is an indication of the adoption of legislative mechanisms such as Directive 2013/40/EU on attacks against information systems. However, given that the Directive “has been criticised for its vague legal obligations” the Member State implementation of its measures has been allowed a large degree of discretion. Nevertheless, given the difficulty in establishing international consensus on this issue, the Directive could provide an important step towards harmonisation (even if it is not in itself the overarching solution).

6.3 Directive 2013/40/EU on attacks against information systems

The Directive 2013/40/EU entirely replaces the provisions of Council Framework Decision 2005/222/JHA of 24 February 2005. Specifically according to Article 1 the “Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.” The Directive must be adopted before the 4th of September 2015. Directive 2013/40/EU has a clear goal towards the harmonisation of minimum standards by ensuring that these types of crimes are punishable by effective, proportionate and dissuasive criminal penalties. It must be noted that this is an important development as substantive harmonisation would allow for clarity in relation to cross-border substantive legal standards for offences as these can vary and may be broad. Nevertheless, these provisions require transposition in the Member States and this raises concerns in relation to harmonisation and divergences and interpretation and could thus lead to disparity. However, given that the focus of this analysis is on access our attention now turns to the procedural harmonisation measures contained in the Directive.

At an EU level the harmonisation of criminal procedural law has been limited due to a lack of competence and as such harmonisation is fragmented. Although the Convention on Cybercrime does contain a section on procedural law (section 2) and thus a degree of harmonisation, the harmonisation is rather limited. For instance there are no rules on the safe storage of information thus implying that there may be disparities and that storage practices in one country may not satisfy those in another hence affecting the information’s evidentiary value. Moreover, there are no comparable measures at an EU level. As such, this also implies that entities investigating cybercrime may not be able to avail of the same tools (depending on their status as a public body with law enforcement competences).

In essence Directive 2013/40/EU aims to increase criminal justice cooperation through two key means:

- strengthening the existing structure of 24/7 contact points, including an obligation to answer within 8 hours to urgent requests (at least in terms of whether the request will be answered, and the form and estimated time of the answer);

---

244 Convention on Cybercrime CETS No.: 185 accessed on 21/01/2015 at: conventions.coe.int/Treatry/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.
• introducing an obligation to collect basic statistical data on cybercrimes.246

The Directive also aims to improve the cooperation between the competent authorities, agencies and bodies (such as national authorities), Eurojust, Europol (and its European Cyber Crime Centre),247 and ENISA. This is indicative of the general move towards more harmonisation and increasing judicial cooperation.

6.4 Directive 2014/41/EC on the European Investigation Order in criminal matters

An additional EU harmonising measure that is significant for this analysis is Directive 2014/41/EC on the European Investigation Order in criminal matters.248 This Directive will replace most of the existing laws regarding the transfer of evidence between Member States from the 22nd of May 2017. However, significantly both Ireland and Denmark have opted out. Currently the legislative framework consists of:

• The Council of Europe Convention on Mutual Assistance in Criminal Matters of 20 April 1959 (and its two additional protocols),249
• Parts of the Schengen Convention;250
• The 2000 EU Convention on Mutual assistance in criminal matters (and its Protocol);251
• the 2008 Framework Decision on the European evidence warrant;252 and
• the 2003 Framework Decision on the execution in the European Union of orders freezing property or evidence (as regards freezing of evidence).253

This new Directive provides a definite step forward as it moves from the notion of legal assistance to mutual recognition. According to Article 1(1)

“A European Investigation Order (EIO) is a judicial decision which has been issued or validated by a judicial authority of a Member State (‘the issuing State’) to have one or several specific investigative measure(s) carried out in another Member State (‘the executing State’) to obtain evidence in accordance with this Directive. The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State.”

247 This Centre has 4 key functions: (1) serve as the European cybercrime information focal point; (2) pool European cybercrime expertise to support Member States; (3) provide support to Member States’ cybercrime investigations; (4) become the collective voice of European cybercrime investigators across law enforcement and the judiciary. For more see: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0140&from=EN; C. O’Donoghue, T.J. Nagle and C. Nielsen Czuprynski, EU Proposed Directive on Network and Information Security, 13 February 2013, http://www.reedsmith.com/EU-Proposed-Directive-on-Network-and-Information-Security-02-13-2013/.
As such the Directive applies to almost all investigative measures but will not apply to Schengen cross-border surveillance by police officers under the Schengen Convention or the setting up/gathering of evidence by a joint investigation team. Indeed, as per recital 8 “the setting up of a joint investigation team and the gathering of evidence within such a team require specific rules which are better dealt with separately.” In essence this mechanism will allow for more effective cross-border investigations which is important in order to identify and prosecute the perpetrators.\textsuperscript{254} Given that there is still quite some time before the Directive must be adopted, progress as regards implementation should be watched with interest.

### 6.5 Conclusion

Public sector access to information stored in the cloud is a topical and controversial topic. Cloud users often are concerned about access and the powers held by public authorities. The disparities between Member States have led to a complex array of national provisions and a lack of harmonised approaches. Moreover, as CLARUS has a clear focus on secure storage, the accessibility of information encrypted using CLARUS processes will further complicate the role of law enforcement authorities. However, although this may seem like a barrier to justice, it is also a manifestation of privacy, confidentiality and data protection. Accordingly, the principle of proportionality has a strong link to this issue.

\textsuperscript{254} E. De Capitani and S. Peers ‘The European Investigation Order: A new approach to mutual recognition in criminal matters’ accessed on 23/04/2015 at: eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html
### 7 Legal and ethical requirements table

From the analysis provided throughout the preceding chapters certain key requirements have been extracted from the analysis. These are presented in tabular format below.

For the purpose of the CLARUS requirements, classifications regarding the importance of requirements have been made:

- **Must have** (MH): the project will be seriously impacted if this requirement is not met.
- **Should have** (SH): a requirement that, if it is not met, seriously impacts the project, but it can be delivered on a different timescale than the must-haves.
- **Could have** (CH): optional requirements which can improve the project outcome and the value of its results, but are not essential to the main delivery (not too many Could-have requirements should be dropped in the design).
- **Would like** (WL): truly optional features which can be delivered if there is sufficient effort available within a task, or if they can be found elsewhere and integrated easily.

It should be observed that all these requirements fit into the ‘Must have’ category and have been marked accordingly.

<table>
<thead>
<tr>
<th>Req. No.</th>
<th>Description</th>
<th>Type</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req. 1.1</td>
<td>Access to datasets</td>
<td>MH</td>
<td>The specific provisions provided in the ACCESS and INSPIRE directives requiring access to the datasets covered must be complied with.</td>
</tr>
<tr>
<td>Req. 1.2</td>
<td>The provision of metadata</td>
<td>MH</td>
<td>The specific provisions as provided for under the INSPIRE Framework (Article 5 INSPIRE Directive and the Metadata Regulation) must be complied with.</td>
</tr>
<tr>
<td>Req. 1.3</td>
<td>Restrictions on access</td>
<td>MH</td>
<td>The specific provisions regarding the restrictions on access, i.e. public access, as provided in the ACCESS and INSPIRE directives must be complied with.</td>
</tr>
<tr>
<td>Req. 2.1</td>
<td>If personal (sensitive) data is processed the specific restrictions should be complied with</td>
<td>MH</td>
<td>The general requirements related to the processing of personal data must be complied with. The more stringent national laws applicable for the processing of sensitive data and the requirements of Art. 8 Directive 95/46/EC (including export restrictions) must be complied with if these special categories of data are being processed.</td>
</tr>
<tr>
<td>Req. 2.2</td>
<td>The data controller is required to have a legal ground in order to process the personal data. Regard should also be had to any potential exemption in national law to the application of the legal requirements.</td>
<td>MH</td>
<td>Article 7 Directive 95/46/EC, and in the case of the exemption Article 13 and the relevant national legislation justifying this exemption.</td>
</tr>
<tr>
<td>Req. 2.2.1</td>
<td>If CLARUS relies on consent as a grounds for processing this must be legally and validly obtained</td>
<td>MH</td>
<td>Article 7(a) Directive 95/46/EC</td>
</tr>
<tr>
<td>Req. 2.2.2</td>
<td>If the performance of a contract is the legal ground for data processing the data controller must only act within the</td>
<td>MH</td>
<td>Article 7(b) Directive 95/46/EC. This could happen if an external entity is used to process personal data.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Description</td>
<td>Reference</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Req. 2.2.3</td>
<td>If the existence of a legal obligation is the legal ground for the data processing, the data controller must only act in accordance with and within the boundaries of the legal obligation. The extent of data processing must be necessary to fulfil the legal obligation.</td>
<td>MH Article 7(c) Directive 95/46/EC.</td>
<td></td>
</tr>
<tr>
<td>Req. 2.2.4</td>
<td>If the legal ground for data processing is the vital interest of the data subject, the data controller must only act to protect these vital interests and the extent of data processing must be necessary.</td>
<td>MH Article 7(d) Directive 95/46/EC.</td>
<td></td>
</tr>
<tr>
<td>Req. 2.2.5</td>
<td>If the legal ground for data processing is the performance of a public interest task or in the exercise of official authority, the data controller must only act in the furtherance of this task.</td>
<td>MH Article 7(e) Directive 95/46/EC.</td>
<td></td>
</tr>
<tr>
<td>Req. 2.2.6</td>
<td>If the legitimate interest of the data controller is used as the legal ground for data processing, the controller is required to have a legitimate interest in the data processing.</td>
<td>MH Article 7(f) Directive 95/46/EC.</td>
<td></td>
</tr>
<tr>
<td>Req. 2.3</td>
<td>CLARUS must respect the Data quality principles.</td>
<td>MH Article 6 Directive 95/46/EC</td>
<td></td>
</tr>
<tr>
<td>Req. 2.3.1</td>
<td>All processing operations involving personal data in CLARUS must be completed fairly and lawfully and cannot contravene the protections afforded under the Data Protection Framework.</td>
<td>MH Article 6(a) Directive 95/46/EC.</td>
<td></td>
</tr>
<tr>
<td>Req. 2.3.2</td>
<td>The personal data must only be processed for specified explicit and legitimate purposes and not further processed in a way incompatible with those purposes.</td>
<td>MH Article 6(b) Directive 95/46/EC.</td>
<td></td>
</tr>
<tr>
<td>Req. 2.3.3</td>
<td>The personal data processing must be necessary and adequate for the purpose specified</td>
<td>MH Article 6(c) Directive 95/46/EC.</td>
<td></td>
</tr>
<tr>
<td>Req.</td>
<td>In order to ensure that the</td>
<td>MH Article 6(d) Directive 95/46/EC.</td>
<td></td>
</tr>
<tr>
<td>Req. 2.3.4</td>
<td>personal data is accurate and up to date the responsible data controller MUST take every reasonable step. As such the accuracy of personal data stored should be constantly assessed an inaccurate data should be deleted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Req. 2.3.5</td>
<td>Personal data MUST be deleted or anonymised when no longer necessary for the specified purpose.</td>
<td>MH</td>
<td>Article 6(d) Directive 95/46/EC</td>
</tr>
<tr>
<td>Req. 2.4</td>
<td>CLARUS should not make automated individual decisions regarding the data subject, unless authorised by law.</td>
<td>MH</td>
<td>Article 15 Directive 95/46/EC</td>
</tr>
<tr>
<td>Req. 2.5</td>
<td>The data controller must ensure the easy operation of the data subject’s rights. This could include the integration of a system capable of processing data subject requests.</td>
<td>MH</td>
<td>Article 14 Directive 95/46/EC</td>
</tr>
<tr>
<td>Req. 2.6</td>
<td>Any transfer of data outside the EEA must respect the specific provisions related to data transfer</td>
<td>MH</td>
<td>Articles 25 and 26 Directive 95/46/EC</td>
</tr>
<tr>
<td>Req. 2.7</td>
<td>Requirements in relation to traffic and location data must be complied with</td>
<td>MH</td>
<td>Articles 5 and 9 Directive 2002/58/EC</td>
</tr>
<tr>
<td>Req. 3.1</td>
<td>Data controller and processor must ensure the implementation of appropriate state of the art technical and organisational measures to ensure security and confidentiality.</td>
<td>MH</td>
<td>Article 17 Directive 95/46/EC and Article 4 Directive 2002/58/EC</td>
</tr>
<tr>
<td>Req. 3.2</td>
<td>The requirements as specified in Directive 2002/58/EC regarding breach notification obligations for public communication network providers must be complied with. Moreover, national legislation on the requirements in relation to breach notification more generally must be consulted.</td>
<td>MH</td>
<td></td>
</tr>
<tr>
<td>Req. 4.1</td>
<td>Once a CSP becomes aware of illegal data being stored on its hardware, the provider must comply with the notice-and-take-down procedures and immediately remove or disable</td>
<td>MH</td>
<td>Article 14 Directive 2000/31/EC</td>
</tr>
<tr>
<td>Req. 5.1</td>
<td>CSPs must comply with national provisions relating to access orders, emanating from public authorities with the competence to make such requests.</td>
<td>MH</td>
<td>Reference should be made to national legislation.</td>
</tr>
</tbody>
</table>
8 Impact of requirements on CLARUS as derived from the use cases

This Chapter of the analysis will provide an application of the legal and ethical requirements examined thus far to the context of CLARUS. This application will rely on the application cases derived in deliverable 2.1 ‘Definition of application cases’. However, it does not provide a comprehensive outline of the discussions provided in D2.1 and reference should be made to this deliverable for a more specific analysis.

Geospatial data application case
Discovering and sharing geo-referenced data is critical for environmental professionals. Therefore, numerous initiatives around the world aim to remove technical obstacles to institutional information sharing and to facilitate the adoption of open, spatially enabled reference architectures in enterprise environments. In this context, the cloud has received an ever-growing interest through its capabilities of addressing common requirements such as huge data volumes, ubiquitous access and quality of services, computation power and economic competitiveness. Nevertheless, CLARUS will investigate certain security issues such as service continuity and access management that could arise in this context, in particular when (sensitive) personal data is at stake.

As CLARUS focuses on the secure storage of data migrated to the cloud, it is important to consider these security expectations related to geospatial data. The following table, as extracted from deliverable 2.1, illustrates these expectations.

<table>
<thead>
<tr>
<th>Security Expectations</th>
<th>Geo Data Demonstration Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geospatial subjects</td>
<td>Refers to §</td>
</tr>
<tr>
<td>Data</td>
<td>accessibility and alteration protection</td>
</tr>
<tr>
<td></td>
<td>metadata-based access limitations</td>
</tr>
<tr>
<td></td>
<td>confidentiality</td>
</tr>
<tr>
<td></td>
<td>authenticity of sources (data quality)</td>
</tr>
<tr>
<td>Services</td>
<td>access authentication (e.g. GeoITM)</td>
</tr>
<tr>
<td></td>
<td>metadata-based access limitations</td>
</tr>
<tr>
<td></td>
<td>secure communication protocols</td>
</tr>
<tr>
<td>Personal Data</td>
<td>personal data protection</td>
</tr>
<tr>
<td></td>
<td>access auditing</td>
</tr>
<tr>
<td>Cloud-based hosting</td>
<td>data location risks</td>
</tr>
<tr>
<td></td>
<td>information system loss of control risks</td>
</tr>
<tr>
<td></td>
<td>multi-tenancy and resource sharing risks</td>
</tr>
</tbody>
</table>

The above table summarises the initial security expectations in relation to the geospatial data application case. It should be noted that for each of the categories, namely data, services, personal data and cloud-
based hosting, there are specific security expectations listed and these relate to the confidentiality and security of the information that is being stored and the restrictions on access. These security expectations are manifestations of legal requirements in relation to the confidentiality of certain spatial and environmental datasets as described in Chapter 2 of this deliverable. In particular, the legal provisions regarding the restrictions on access as provided by the ACCESS and INSPIRE directives stipulate conditions and scenarios in which the publication of the datasets relevant for these legislative measures are restricted and prevented from being made public. Moreover, the metadata requirements as foreseen by the INSPIRE framework provide detailed obligations regarding the outlining of specific key factors, for example the access levels relevant to a particular piece of information. These same provisions also stipulate requirements in relation to the quality and reliability of the sources as discussed in Chapter 2.

As may be apparent, the geospatial data being used in the context of CLARUS may not necessarily contain personal data. However, such information may be used in relation to the restriction of access that would be given to particular datasets. More precisely, personal data of the individuals authorised to access the data or service may be collected in order to verify the authenticity of the access request. As such, such access controls may require identity management procedures (i.e. registration, identification, authentication, and the administration of rights and privileges). Accordingly, such processing of personal data needs to comply with the detailed requirements provided in the analysis in Chapter 3.

As described in D2.1, in the context of geospatial data three main demonstration cases have been outlined, namely:

- Storage of geospatial data
- Publication and processing of geospatial data
- Collaboration on geospatial data

In relation to each of these demonstration cases, it must be noted that the ACCESS and INSPIRE directives provide a unique framework for the publication of publicly held datasets. The requirements from a legal perspective thus relate to (1) the publication of this information, (2) the access limitations and (3) the particular format and obligations specifically related to the storage (i.e. the metadata obligations). Regarding the second of these, as examined supra, the privacy and data protection framework has relevance. Therefore, one must also consider the restrictions contained therein. The following table provides a detailed representation of the specific legal requirements relevant for the application to the demonstration cases.

<table>
<thead>
<tr>
<th>Applied Req.</th>
<th>Description</th>
<th>Relevant general req.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AReq. 1.1</td>
<td>The implementation of the CLARUS solution must integrate all specific requirements as stipulated in the ACCESS and INSPIRE directives in relation to the limitations on access and the provision of certain information, i.e. metadata.</td>
<td>Req. 1.1-1.3</td>
</tr>
<tr>
<td>AReq. 1.2</td>
<td>Where personal data is processed, all privacy and data protection requirements must be complied with and in the context of the geospatial data use case, this has particular relevance for access controls.</td>
<td>Req. 2.1-3.2</td>
</tr>
</tbody>
</table>
8.1 eHealth data application case

Since there is a growing demand for increased storage capacity by big hospitals, the latter regularly use cloud storage services to cover these growing needs. However, the security issues related to the use of cloud services to store this highly sensitive personal data are pressing, as CSPs cannot assure the integrity and confidentiality of the datasets they store. Therefore, CLARUS chose eHealth as an application case, to analyse the possibility of a layer on top of a cloud storage to ensure security of these sensitive medical records.

Specifically, as contained in D2.1, there are clear expectations regarding the assurance of the preservation of the integrity, confidentiality and accessibility of the passive medical records stored in the cloud data storage space using the CLARUS solution. Given the sensitivity of the information being stored regarding the eHealth application case, the specific security provisions as contained in the DPD play a key role. Accordingly, access controls and the maintenance of security protocols are key concerns in this context. As provided by D2.1, the only expectation of the CLARUS framework in the context of eHealth data is to guarantee the security and privacy of all the passive medical health records stored in the cloud service via the encryption, masking and/or anonymisation of the data transferred to the cloud and of course its decryption, unmasking and de-anonymisation when accessed and retrieved. In particular, four main demonstration cases are described in detail in relation to the eHealth application case, namely:

- Storage of passive medical health records
- Access and retrieval of passive medical health records
- Advanced queries on structured data contained in passive medical health records
- Statistical computation on structured data contained in passive medical health records

In relation to the first and second of these demonstration cases, the key consideration from a legal perspective is the secure storage and the restriction on access of the specified medical records. This is a particular reference to the security of sensitive personal data as provided for in Article 17 DPD. In relation to the third and fourth demonstration cases, the data protection principles should be considered more closely. For instance, data minimisation and purpose specification and limitation (as described in section 3.3.4) have particular relevance. Indeed, one should refer to the specific considerations outlined in relation to the privacy by design principle and its implementation as described in section 3.5.2.1. The following table provides a representation of the specific legal requirements relevant for the application to the demonstration cases.

<table>
<thead>
<tr>
<th>Applied Req.</th>
<th>Description</th>
<th>Relevant general req.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AReq. 1.1</td>
<td>Specifically in relation to the eHealth data use case, the requirements in relation to the secure storage of sensitive health information must be complied with, and relevant access controls must be implemented.</td>
<td>Req. 2.1-3.2</td>
</tr>
<tr>
<td>AReq. 1.2</td>
<td>Where personal data is processed, in order to ensure the authentic nature of an access request, all privacy and data protection requirements must be complied with.</td>
<td>Req. 2.1-3.2</td>
</tr>
</tbody>
</table>
8.2 Legal Requirements for governmental entities

In the sections above we provided the applicable legal requirements for CLARUS in general (section 7), as well as in the context of the geospatial application case (section 8.1.) and the eHealth data application case (section 8.2). Following Recommendation N. 7 of the Interim Review, according to which “further refinement of requirements is needed, e.g., with respect to identification of adequate level of technical and organisational measures for security and confidentiality required for specific use cases”, this section will provide the legal requirements in the context of other governmental organisations to which CLARUS may apply.

The data protection legislation applies to both public and private entities, hence, the above mentioned legal requirements are also applicable when CLARUS is used by other governmental administrations. However, additional and more specific requirements need to be taken into consideration according to the type of the organisation, the type of personal data processed and the ad hoc applicable national laws. In this respect, we will provide as examples of such governmental organisations the legal requirements to be taken into consideration by hospitals and in particular the hospitals in Spain, as well as the example of public finance entities, and in particular the national Bank of Spain.

To this end, we will first outline the overview of the applicable legal framework for these governmental organisations. Furthermore, we will identify a set of other governmental organizations that could be potential target users interested in CLARUS. Moreover, we will demonstrate the particularities of these organisations and finally, we will extract generic requirements as a factorization of those specific requirements.

I. Overview of the legal framework

As thoroughly described above, whenever personal data are processed, then the data protection legislation will apply, including thus whenever personal data are encrypted. As a reminder, Directive 95/46 is transposed into the national legislations of each EU Member State and thus, currently there is no harmonised data protection legislation across the EU. Therefore, different governmental organisations across Europe will have to abide by their national specific legal requirements. The following table demonstrates how the European legal requirements have been transposed into the national legislation of Spain in the context of the demonstration cases of hospitals and public finance entities.

<table>
<thead>
<tr>
<th>Legal and regulatory framework</th>
<th>National laws – the example of a public hospital in Spain</th>
<th>National laws - the example of public finance entities, the National Bank of Spain</th>
</tr>
</thead>
<tbody>
<tr>
<td>- European Convention on Human Rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Charter of Fundamental Rights of the European Union</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Directive 95/46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- General Data Protection Regulation (into force 25 May 2018)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ePrivacy Directive 2002/58/EC (under revision)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
II. Specific legal requirements for governmental organisations

The notion of a ‘public authority of body’ is a notion to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.\textsuperscript{255} Also, a public task may be carried out not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, in sectors such as, according to national regulation of each Member State, public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.\textsuperscript{256}

Among the potential governmental customers of CLARUS, such as public finance entities, educational institutions and healthcare centers, we will focus our analysis to those imposing the stricter restrictions and processing sensitive data the most. To this respect, we will demonstrate the specific legal requirements that hospitals and public finance entities in Spain have to abide by.

A. Hospitals – the example of hospitals in Spain

As already described in detail in this deliverable as well as in the Addendum of D2.4, the protection of health related data is incumbent on national laws both under the current and upcoming legal regimes. In this respect, the following table will outline the data protection and security legal requirements that hospitals in Spain are required to abide by in order to use cloud services.

| Directive 95/46/EC\textsuperscript{257} was transposed into the national legislation of Spain by the Organic Law 15/1999 of 13 December 1999 on the Protection of Personal Data.\textsuperscript{258} Article 9 of the Organic law lays down the security requirements for processing personal data, further implemented in Articles 79 of the Royal Decree.\textsuperscript{259} These requirements are applicable both to controllers (in this case, the hospital) and processors (cloud providers) and are extracted from the above mentioned provisions. To this end, the following requirements specify and refine the ones provided in D.2.4. At this point, it is important to mention that the Royal Decree identifies three levels of security for processing of personal data: basic, medium and high security levels. The latter applies to data referring to health—among other categories, which are relevant for the CLARUS eHealth use case. The following table


\textsuperscript{257} 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, further implemented in Articles 79 of the Royal Decree.\textsuperscript{259} These requirements are applicable both to controllers (in this case, the hospital) and processors (cloud providers) and are extracted from the above mentioned provisions. To this end, the following requirements specify and refine the ones provided in D.2.4. At this point, it is important to mention that the Royal Decree identifies three levels of security for processing of personal data: basic, medium and high security levels. The latter applies to data referring to health—among other categories, which are relevant for the CLARUS eHealth use case. The following table


summarises the key legal requirements to be implemented by a hospital when using cloud services in Spain.

Table 1 Legal Requirements for the use of cloud by hospitals in Spain

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
</tr>
</thead>
</table>
| **R1. Incident recording and notification (Articles 90 and 103 of the Royal Decree)** | The hospital, as data controller (as well as the data processor-cloud provider) should:  
- Have in place a procedure for notification and management of incidents affecting personal data;  
- Have in place a procedure for recording incidents in a register (type of incident, when it occurred, if it was detected, who notified the incident, to whom it was communicated, the effect of it and the applied mitigating measures, the procedures for the recovery of data, the person who executed the process, the data restored and, if appropriate, which data have had to be manually recorded in the recovery process);  
- Keep a record, in addition to the above-mentioned for at least two years attempts to access data; for each attempt to access the data, at least the following shall be stored: identification of the user accessing the data, the date and time it was accessed, the filing system accessed, the type of access and whether it has been authorized or denied;  
- Audit the information systems and processing and data storage installations at least every two years, to verify compliance with the requirements of the Royal Decree. |
| **R2. Access control (Article 91 of the Royal Decree)** | Users (doctors etc.) shall only have access to those resources required for the performance of their functions. In this regard, the hospital is required to:  
- Keep an updated list of users and user profiles, and the authorized accesses for each one;  
- Establish mechanisms to avoid a user being able to access resources with rights other than those authorized;  
- Ensure that only staff members authorized in the security document shall grant, alter or annul the access authorized to resources, pursuant to the criteria established by the data controller;  
- Ensure that any person having access to the resources shall be subject to the same security conditions and obligations as the internal personnel;  
- Ensure that only the personnel authorized in the security document shall have access to the places housing the physical equipment that supports the information systems;  
- Make certain that suitable and adequate access control measures are put in place that ensure the confidentiality of patient data, ensuring that users access only healthcare data that they are allowed to access based on their authentication and access levels, that different access types are embedded where the patient and doctors can give only view, view and write permissions and revoke these permissions when needed. |
| **R3. Management of supports and documents (Article 92 and 97 of the Royal Decree)** | The hospital should:  
- Permit identification of the type of information contained in the supports and documents containing personal data;  
- Allow an inventory (except when the physical characteristics of the support makes it impossible);  
- A registration for the entry and departure of supports or documents containing personal data;  
- The identification of supports should be achieved through logical labelling systems allowing users with authorized access to identify their contents. |
| **R4. Identification and authentication (Article 93 and 99 of the Royal Decree)** | The hospital has to guarantee the correct identification and authentication of the users  
- When the authentication mechanism is based on the use of passwords, there shall be a procedure of disclosure, distribution and storage guaranteeing confidentiality and integrity;  
- Frequent change of passwords should be established (no less than yearly);  
- Passwords shall be stored in an unintelligible way (for example, encryption);  
- A mechanism to limit the possibility of repeated attempts of unauthorized access to the information systems should be established. |
| **R5. Backup copies and recovery (Article 94 (1) and 102m of the Royal Decree)** | Backup copies of personal data to be made at least weekly, unless data has not been updated in the meantime.  
- Similar procedures are required for recovery of data at the moment of loss or destruction;  
- Whenever backups are created, the copy must be kept in a different physical location than the installation housing the infrastructure hardware processing the data. |
| **R6. Security of communications network** | The transfer of personal data through public or wireless electronic communications networks shall guarantee that the information shall not be intelligible or manipulated by third parties (i.e. by encrypting communications through such networks). |
| **R7. Consent as a legal basis** | If the patient’s consent is used as a basis for using the CLARUS functionalities, the consent has to fulfill certain conditions. For consent to be valid it should be freely given, specific and informed.  
- Whenever the summary record is absolutely voluntary, and the patient will still receive treatment whether or not he or she has consented to the creation of a summary record, the consent is deemed to be freely given because the patient will suffer no disadvantage if consent is not given or is withheld;  
- Whenever there is a financial incentive to choose the e-health record (a moderate one), the consent is deemed to be freely given because the patient refusing the e-health record does not suffer disadvantage;  
- Whenever patients refusing the e-health system have to pay a substantial extra cost compared to the previous tariff system and the processing of their file is considerably delayed, the consent cannot be deemed to be freely given because it creates a clear disadvantage for those not consenting. Thus, another legitimate ground(s) to process sensitive data is necessary in this case, such as the ‘legitimate interest’ of the data controller.261 |
| **R8. Storage of clinical records** | Health centers shall keep clinical documentation in adequate conditions that guarantee their maintenance and security to ensure assistance to the corresponding patient as long as required.  
- In any case, such documentation should be kept for a period of 5 years as from the date the patient was discharged.  
- Should enable the storage of such records up to 5 years, when necessary. |
| **R9. Protection of patients’ rights** | Enhance user choice and facilitate the protection of privacy rights of the data subjects (i.e. whenever a patient data is disclosed to another doctor for a second opinion, the patient is notified of such access automatically). |
| **R10. Confidentiality** | Doctors are bound by medical secrecy, meaning they must keep confidential any information either revealed by a patient or which they have found out as a consequence of their activities.  
- This duty does not end with the patient’s death and doctors only may be exempted from this obligation under exceptional circumstances (e.g., notifiable diseases, by virtue of a legal or judicial obligation at the request of a judicial authority, etc.).  
- Furthermore, doctors in charge of a healthcare center/service must ensure that privacy and confidentiality of health data are not compromised.  
- Health and administrative data must be clearly separated.  
- Doctors must require their staff, regardless whether they are healthcare professionals or not, to comply with the aforesaid confidentiality obligations.  
- It is possible to show medical cases photographed or filmed for academic purposes or in order to disseminate for scientific knowledge, provided the patient has given his express consent first or when his anonymity is ensured. |
| **R11. Integrity, Confidentiality, Authenticity and Traceability** | Three communities have been defined depending on the level of the security requirements provided to the CSP.262  
- Low community:  
  - The creation, move, activation and destruction of virtual elements will be registered. Likewise the assembly and removal of physical or virtual information media will be registered too. |

---


261 Law 41/2002 of 14 November 2002 on the Autonomy of the Patient and the Rights and Obligations with regard to Information and Clinical Documentation (the “Patients’ Rights Law”)

B. Public finance entities - the example of the National Bank of Spain

In this subsection, we will demonstrate the applicable legal requirements that a public finance entity in Spain should abide by, as an example of another governmental organisation that CLARUS would apply. In particular, we will provide the example of the Bank of Spain (Banco de España), which is the national central bank and the supervisor of the Spanish banking system.


<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security components (like DMZ, firewalls or proxies) will not be hosted in the same machine with production components.</td>
</tr>
<tr>
<td>The physical network perimeter supporting the community will meet the requirements of CCN-STIC-811 standard.</td>
</tr>
<tr>
<td>Identification and authentication requirements from the hypervisor administrator will be the same as a Medium community system according to the National Security Schema.</td>
</tr>
<tr>
<td>Base machines will not be shared with other communities.</td>
</tr>
<tr>
<td>The same hypervisor will not be shared with other communities.</td>
</tr>
<tr>
<td>The hypervisor administration will be separated from virtualized elements administration.</td>
</tr>
<tr>
<td>Identification and authentication requirements from the hypervisor administrator will be the same as a High community system according to the National Security Schema.</td>
</tr>
<tr>
<td>The administration network will be separated logically or physically from the from other communities administration network.</td>
</tr>
<tr>
<td>Requirements</td>
</tr>
<tr>
<td>--------------</td>
</tr>
</tbody>
</table>
| **R1. Incident recording and notification**<br>(Article 90 and 100 of the Royal Decree) | The data controller (in this case, the bank), as well as the data processor (the cloud provider) should:  
- Have in place a procedure for notification and management of incidents affecting the individuals’ personal data;  
- Have in place a procedure for recording incidents in a register (for recording the type of incident, when it occurred, if it was detected, who notified the incident, to whom it was communicated, the effect of it and the applied mitigating measures).  
- Provide the procedures for the recovery of data, indicating the person who executed the process, the data restored and (if appropriate) which data have had to be manually recorded in the recovery process. Authorisation of the data controller shall be necessary for the execution of the data recovery procedures. |
| **R2. Access control**<br>(Article 91 of the Royal Decree) | Users shall only have access to those resources required for the performance of their functions. In this regard, the data controller is required to:  
- Keep an updated list of users and user profiles, and the authorized accesses for each one;  
- Establish mechanisms to avoid a user being able to access resources with rights other than those authorized;  
- Ensure that only staff members authorized in the security document shall grant, alter or annul the access authorized to resources, pursuant to the criteria established by the data controller;  
- Ensure that any person having access to the resources shall be subject to the same security conditions and obligations as the internal personnel.  
**Physical Access Control**  
- Only the authorised personnel in the security document shall have access to the places housing the physical equipment that supports the information systems. |
| **R3. Management of supports and documents**<br>(Article 92 of the Royal Decree) | The data controller should:  
- Permit identification of the type of information contained in the supports and documents containing personal data;  
- Allow an inventory (except when the physical characteristics of the support makes it impossible);  
- A registration for the entry and departure of supports or documents containing personal data;  
- Erase or destroy any document or support containing personal data that is to be discarded by taking measures aimed at avoiding access to the information contained therein or its later recovery;  
- The identification of supports containing personal data that the organisation deems particularly sensitive may be made through logical labelling systems allowing users with authorized access to identify their contents. |
| **R4 Identification and authentication**<br>(Article 93 of the Royal Decree) | The data controller has to guarantee the correct identification and authentication of the users  
- When the authentication mechanism is based on the use of passwords, there shall be a procedure of disclosure, distribution and storage guaranteeing confidentiality and integrity;  
- Frequent change of passwords should be established;  
- Passwords shall be stored in an unintelligible way (i.e. encryption);  
- A mechanism to limit the possibility of repeated attempts of unauthorized access to the information systems should be established. |
| **R5. Backup copies and recovery**<br>(Article 94 of the Royal Decree) | Backup copies of personal data to be made at least weekly, unless data has not been updated in the meantime.  
- Similar procedures are required for recovery of data at the moment of loss or destruction;  
- The data controller shall ensure verification every six months of the correct definition, operation and application of the procedures for making backup copies and for the recovery of data;  
- The tests prior to the implementation or amendment of the information systems the process filing systems with personal data shall not be done with real data, unless the relevant level of security for the processing is ensured and it is recorded in the security document. If tests are to be done with real data, a backup copy shall be made first. |
<table>
<thead>
<tr>
<th>R6. Appointment of security officers</th>
<th>The security document shall appoint one or several security officers commissioned with coordinating and monitoring all above mentioned measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Article 95 of Royal Decree)</td>
<td>• for all the filing systems or processing of personal data or specific depending on the information systems used;</td>
</tr>
<tr>
<td></td>
<td>• his/her activities will be clearly recorded in the security document;</td>
</tr>
<tr>
<td></td>
<td>• this designation does not imply an exemption of the data controllers’ or data processors’ liability.</td>
</tr>
<tr>
<td>R7. Audit</td>
<td>The information systems and processing and data storage installations shall be subject, to internal or external audit, at least every two years</td>
</tr>
<tr>
<td>(Article 96 of Royal Decree)</td>
<td>• Or whenever substantial amendments to the information system that may have repercussions in the fulfillment of the implemented security measures are made</td>
</tr>
<tr>
<td></td>
<td>• The audit report shall report on the adaptation of the measures and monitoring to the regulations, identifying deficiencies and proposing the corrective or complementary measures (as well as data, facts and observations and proposed recommendations);</td>
</tr>
<tr>
<td></td>
<td>• The audit reports shall be analysed by the competent security officer, who shall inform the data controller of the conclusions, to be made available to the Spanish Data Protection Agency</td>
</tr>
<tr>
<td>R8. Outsourcing</td>
<td>Requirements for outsourcing in the context of financial services or bank’s internal activities</td>
</tr>
<tr>
<td>(Bank of Spain Circular 3/2008)</td>
<td>• “internal control capacities of the institutions themselves do not see diminished as a result of the outsourcing;</td>
</tr>
<tr>
<td></td>
<td>• the monitoring capabilities of the Bank of Spain will not see impaired as a result of the delegation;</td>
</tr>
<tr>
<td></td>
<td>• the contracting of services or functions may not result in interference with the supervisory powers of the Bank of Spain, and so must be provided in contracts, whatever the area of activity; to this end, they must include in them a clause providing direct access without restrictions the Bank of Spain to the information in the credit institution held by providers as well as the ability to check in their premises themselves, the adequacy of the systems, tools and applications used in the provision of services or delegated functions”;</td>
</tr>
<tr>
<td></td>
<td>• The financial entities have to present their supervisors, BdE or the Central European Bank, all relevant documentation, including risk assessments.</td>
</tr>
<tr>
<td></td>
<td>The Bank of Spain has authorised cloud providers to provide non-essential services such as an emailing system, after a comparative risk assessment.</td>
</tr>
<tr>
<td>R9. Integrity, Confidentiality, Authenticity and Traceability</td>
<td>Three communities have been defined depending on the level of the security requirements provided to the CSP.</td>
</tr>
<tr>
<td></td>
<td>Low community:</td>
</tr>
<tr>
<td></td>
<td>• The creation, move, activation and destruction of virtual elements will be registered. Likewise the assembly and removal of physical or virtual information media will be registered too.</td>
</tr>
<tr>
<td></td>
<td>• Security components (like DMZ, firewalls or proxies) will not be hosted in the same machine with production components.</td>
</tr>
<tr>
<td></td>
<td>• The physical network perimeter supporting the community will meet the requirements of CCN-STIC-811 standard.</td>
</tr>
<tr>
<td></td>
<td>• Identification and authentication requirements from the hypervisor administrator will be the same as a Medium community system according to the National Security Schema.</td>
</tr>
<tr>
<td></td>
<td>Medium community: In addition to the Low community requirements</td>
</tr>
<tr>
<td></td>
<td>• Base machines will not be shared with other communities.</td>
</tr>
<tr>
<td></td>
<td>• The same hypervisor will not be shared with other communities.</td>
</tr>
<tr>
<td></td>
<td>• The hypervisor administration will be separated from virtualized elements administration.</td>
</tr>
<tr>
<td></td>
<td>• Identification and authentication requirements from the hypervisor administrator will be the same as a High community system according to the National Security Schema.</td>
</tr>
</tbody>
</table>


### High community: In addition to the Medium community requirements

- The administration network will be separated logically or physically from the other communities administration network.

The above mentioned requirements for the Bank of Spain are applicable to the public finance entities located in Spain. As already described above, Directive 95/46 is transposed into the national legislations of each EU Member State. Thus, currently there is no harmonised data protection legislation across the EU. Therefore, other financial institutions in Europe will have to abide by their own specific national legal requirements. Furthermore, as stated in Addendum to D2.4, this situation will change with the coming into force of the GDPR on 25 May 2018, since the Regulation is directly applicable and does not have to be transposed into national laws, aiming to a strong harmonization within the EU.  

### III. Derived generalized requirements

From the above mentioned examples, it can be concluded that when CLARUS will be applied into different governmental organizations within the EU, the following parameters have to be taken into consideration.

**Parameters:**

1. The national transpositions of Directive 95/46 (MS laws can pose additional requirements)
2. Procedural approvals / authorizations required by national competent authorities (i.e. national Data Protection Authorities, Ethical Committees)
3. Non-binding Guidelines per sector of activity should be taken into consideration

In particular regarding the second parameter, namely the procedural approvals / authorizations required by national competent authorities, such as from national Data Protection Authorities, Ethical Committees etc. and with regard to the reviewers recommendation on the first review meeting, according to which “the specific requirements of some of the targeted user groups, e.g. accreditation / certification requirements related to governmental users, are not adequately discussed in the existing deliverables. This is potential important shortcoming when considering adoption of security-related products within public sector and is surprising, since these issues are closely related to compliance, which is one of the areas addressed within the project”, the following paragraph will address these issues.

Regarding the personal data in the cloud computing services, as mentioned above, under the current regime of the 95/46 Directive, the different Member States within the EU have transposed diverging legislations and have imposed direct (explicitly prescribed by law) and indirect (implied by legal provisions) localisation restrictions, such as that the financial data must be stored locally (see also the table of requirements in Spain for the financial sector above). Prior authorisations and/or notifications for

---

270 The aim of the GDPR is to harmonise the legal framework. However, Member States’ laws are allowed to diverge from the Regulation, but only when explicitly foreseen (employment data, health related data, data for scientific/historical research). For example, with regard to the processing of sensitive data, the Regulation ‘provides a margin of manoeuvre for Member States’ to restrict or specify its rules. For example, Member States are allowed to specify or introduce further conditions for the processing depending, inter alia, on the nature of the data concerned, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL, Recitals 8,10,53; see also p. 5 Addendum of D2.4.

271 On 25 May 2018 the GDPR will be directly applied in all EU member states, thus any national requirements for notifications and/or authorizations will automatically cease to exist; see also Addendum to D2.4.
collection, processing and storing data will become obsolete on May 2018, when the adopted GDPR\textsuperscript{272} will enter into force. With regards to the non-personal data (such as anonymised data), there is currently no comprehensive legal framework regulating these localisation restrictions. However, according to the European Free Flow of Data Initiative, which is one of the Digital Single Market Strategy\textsuperscript{273} (DSM) actions, the EC undertook the EC Data Inception Impact Assessment\textsuperscript{274} (IIA) which highlighted the following problem drivers: a) the diverging data location restrictions and approaches in the Member States in specific sectors or situations; b) the lack of European defined standards and practices on network, information security, prevention and investigation; and c) self-imposed data location restrictions by commercial users in light of the existing legal uncertainty and transparency. According to the recently adopted Communication “Building the European Data Economy”\textsuperscript{275} and its accompanying Staff Working Document\textsuperscript{276}, the EC is currently in the process of beginning structured dialogues with the Member States in order to launch infringement proceedings for unjustified or disproportionate data location measures\textsuperscript{277} and will also take further initiatives.

Whilst the above mentioned parameters need to be considered whenever defining legal considerations for the use of cloud services by governmental entities, some generalized requirements can be however extracted. At this point, it is important to remind that the requirements provided in section 7 of this deliverable do apply and that the following table only demonstrates some generalized conditions as derived from the provided examples.

<table>
<thead>
<tr>
<th>Derived Generalized Requirements</th>
<th>Description</th>
<th>Connection to the specific requirements of the governmental entities examples</th>
</tr>
</thead>
</table>
| Req. 1. Incident recording and notification | Have in place a procedure for notification and management of incidents effecting the individuals’ personal data. | R1-Hospital in Spain  
R1-National Bank of Spain |
| Req. 2. Access control | Have in place an authentication and authorisation mechanism to ensure the authentic nature of an access request. | R2-Hospital in Spain  
R2-National Bank of Spain |
| Req.3. Technical and organisational measures for security and confidentiality | The transfer of personal data through public or wireless electronic communications networks shall guarantee that the information shall not be intelligible or manipulated by third parties, such as an encryption mechanism.  
-Encryption keys should not be stored on Cloud or used on applications running on Cloud. | R6-Hospital in Spain  
R4- National Bank of Spain |


CRUD operations related to users and their permissions should never be performed from a Cloud environment.
- User activity registries should not be provided to the Service Provider.
- Electronic signature and similar services should be executed not using the Cloud by specialized and trusty organisations according to the current laws.278

In particular regarding the identification of adequate level of technical and organisational measures for the security and confidentiality, it is important to emphasise that this is a case by case consideration. In other words, the appropriateness of these measures depends on the type of the personal data processed and can be assessed by undertaking risk assessments, according to the state of the art.279 Measures to address these risks include the use of techniques, such as encryption, pseudonymization, or anonymization.

8.3 Conclusion

From the analysis provided in this chapter, we have identified certain key applied requirements. However, it should be noted that for a successful application of the identified general requirements guidance on their implementation is required throughout the project lifecycle. To this end, these requirements have been updated in Addendum to D2.4 taking into account the changes introduced by the GDPR. In the following section, certain preliminary guidelines for the implementation of a privacy compliant CLARUS solution are outlined. Before delving into these guidelines, it is also worth mentioning that the requirements stipulated in the liability of intermediaries’ discussion also have significance.


279 Article 17 Directive 95/46/EC; see also Article 35 GDPR on Data Protection Impact Assessments.
## 9 Implementation guidelines

Following the above discussion the table provided *infra* indicates some key recommendations for the implementation of the legal requirements in the CLARUS solution. These implementation guidelines have been deciphered from the analysis provided. These are particularly focused on the privacy and data protection considerations. Following the reviewers’ recommendation n.5 on the 1st review meeting, according to which “*further refinement of the implementation guidelines is needed*”, we have updated the following table as follows.

<table>
<thead>
<tr>
<th>Guide. No.</th>
<th>Description</th>
<th>Associated Req.</th>
<th>Implementation suggestions</th>
</tr>
</thead>
</table>
| Guid. 1   | Authentication protocols with privacy features should be implemented.        | Req. 3.1-3.2    | -To have in place an intra-proxy access policy management so that the security manager can define the access rights of the users on the storage/processing services and to define the permissions of the users on the outsourced datasets;  
-To have in place an inter-proxy communication, in order to define the access rights and key exchanges, so that external CLARUS proxies can access the data and request to perform operations on this data;  
-To have in place a VPN connection between CLARUS proxies that use a key to encrypt the requested data, so that only the authorised external proxy can decrypt the data. |
| Guid. 2   | The security of the personal data should be protected throughout the data lifecycle | Req. 3.1-3.2    | -To have in place a security policy management tool that allows defining what to protect and how to protect it; that is, to specify the security requirements;  
-To protected personal data either via anonymisation or encryption during the entire lifecycle of data outsourcing consistently with the security policies. |
| Guid. 3   | Personal data should be securely disposed of at the end of its life-cycle or anonymised in compliance with the limited retention and data minimisation principles. | Req. 2.3.1-2.3.5 | -To have in place a disposal management policy that is transparent to the end users, either by deleting the data or by irreversibly anonymising them.                                                                          |
| Guid. 4   | All communications should be encrypted                                         | Req. 3.1-3.2    | -To have in place mechanisms assuring that the communications between authenticated users and the CLARUS adopting CSP are properly encrypted and that all communications are handled over encrypted channels in the untrusted domains, specifically, between CLARUS CSPs. |
| Guid. 5   | Systems should be designed to ensure that even where personal data are transmitted, any data elements which are not necessary to fulfil the purpose of the transmission are | Req. 2.3.1-2.3.5, 3.1-3.2 | -To implement data protection mechanisms (e.g., data anonymization, data splitting) consistent with the privacy requirements stated in the security policies and the functional needs of the service, so that only the data (e.g., attributes) needed to fulfil the service are transmitted, specifically, between different CLARUS proxies. |
| Guid. 6 | Systems should be designed so as to allow access to the transferred personal data only to the extent necessary for the role being performed. | Req. 2.3.1-2.3.5, 3.1-3.2 | -To have in place an intra-proxy access policy management so that the security manager can define the access rights of the users on the storage/processing services and to define the permissions of the users on the outsourced datasets; -To limit the access and transmission of the data toward the CSP and between CLARUS proxies to the data that is strictly needed to fulfil the service. |
10 Conclusion

From the analysis provided in this deliverable detailed legal and ethical requirements have been outlined and applied to the context of the application cases thereby distilling applied requirements resulting in the creation of guidelines for the implementation of a legally compliant CLARUS solution. To conclude the work completed it should be noted that in order for the implementation of a legally compliant CLARUS solution, partners must give detailed consideration to the obligations outlined in this report. These specified requirements will form the continuing basis of KUL’s work in Task 6.2 ‘Guidance on compliance with legal obligations’ and more specifically D6.3 ‘Legal assessment and recommendations’.
11 References

11.1 Legislation


Council of Europe, Recommendation of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, CM/Rec (2010)13, http://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec%282010%2913E_Profiling.pdf


11.2 Case Law


European Court of Justice C-92/09 and C-93/09, Volker und Markus Schcke GbR and Hartmut Epert v. Land Hessen, 9 November 2010, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130def25239d3960447e4ba36ccf08860afa7.e34KaxiLc3eQc40LaxqMbn4ObxyMe0?text=&docid=79001&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=147217


11.3 Opinions


11.4 Publications


Cronin, K., Best practices and the state of information security, Chicago-Kent Law Review, 2010


Flanagan, A., The law and computer crime: Reading the Script of Reform, International Journal of Law and Information Technology, Volume 13, Issue 1

IDATE, TNO, IViR, User-Created Content: Supporting a Participative Information Society, Study for the European Commission (DG INFSO), December 2008


Janssen, K., The EC Legal Framework for the Availability of Public Sector Spatial Data: An examination of the criteria for applying the directive on access to environmental information, the PSI directive and the INSPIRE directive, Doctoral dissertation in law, 4 December 2009, KU Leuven


Kuczerawy, A. and Ausloos, J., Case Study: European Union & Google Spain, NOC Report on Internet Intermediaries Liability, forthcoming


Sluijs, J.P., Larouche, P. and Sauter, W., Cloud Computing in the EU Policy Sphere, *JIPITEC* 2012/1


Van Alsenoy, B., Kuczerawy, A. and Ausloos, J., Search engines after Google Spain: internet@liberty or privacy@peril?, *ICRI Working Paper Series*, issue 15/2013, 6 September 2013


Walker-Osbourne, C. and Norris, E., Staying one step ahead, *IT Now December 2013*