FP7-INFRASTRUCTURES-2012-1

Grant Agreement no. 312845

Scoping Study for a pan-European Geological Data Infrastructure

D 5.1

Report on trust and authentication

Deliverable number	*D5.1*
Dissemination level	*Public*
Delivery date	*25/08/2013*
Status	*Final*
Author	*Katleen Janssen, Jos Dumortier (KU Leuven)*

Table of Contents

Table of Contents 3

1 Introduction 5

2 Elements of trust in the EGDI 8

2.1 Trust in the data 8

2.1.1 Metadata 8

2.1.2 Quality assessment and assurance procedures 9

2.1.3 Authoritative data or authentic sources 10

2.1.4 Security of the data in the EGDI 11

2.1.5 Impact on the EGDI 14

2.2 Trust in the services..15

2.2.1 Metadata and quality information 15

2.2.2 Service level agreements 15

2.2.3 Security 16

2.2.4 Digital rights management..16

2.2.5 Impact on the EGDI 17

2.3 Trust in the people 18

2.3.1 Identity management 19

2.3.2 Identity management in cross-border transactions 20

2.3.3 The E-signatures directive..21

2.3.4 Revision of the E-signatures directive 22

2.3.5 Federated identity management..23

2.3.6 Personal data protection..25

2.3.7 Impact on the EGDI 32

3 Moving the EGDI to the cloud 34

3.1 The cloud 34

3.2 Benefits of the cloud 35

3.3 Risks of the cloud 36

3.3.1 Security and continuity 36

3.3.2 Personal data protection....38
3.3.3 Control and ownership....39
3.3.4 Interoperability and portability....39
3.3.5 Audits....40
3.3.6 Jurisdiction and applicable law....40
3.4 Impact on the EGDI....41
3.5 Case study: Google....42
3.5.1 Submitting content to Google....42
3.5.2 Using Google services....44
3.5.3 Impact on the EGDI....48
4 Conclusion and summary....49
5 References....52

1 Introduction

The importance of trust in any relationship cannot be denied. This is also the case for any relationship between a data or service provider and its users, whether these users are individual citizens, companies or other public authorities. As a general principle, trust involves one person taking a risk to confide in another person, hoping to benefit from this relationship.[1] In the information society, the concept of trust has broadened its scope from solely inter-human relationships to interactions between technology, devices, systems and users. This is also referred to as computational trust.[2]

There is no one single legal definition of trust. From a legal point of view, trust involves different aspects, not all of which are relevant in the framework of EGDI-Scope.[3] It can relate to legitimate expectations that parties in a relationship can have, for instance in the negotiation phase of a contract.[4] It can also be linked to evidence law and the legal validity of evidence: this is based on a sort of trust in the ability of established and formal criteria to determine whether evidence is trustworthy (e.g. a signed contract has an accepted evidence value, while other documents or witness declarations may have less value). For electronic documents and digital data, the evidence value still remains under discussion.

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 this deliverable we provide an overview of the issues and provisions relating to trust that need to be taken into account in the context of the sharing of geological data and the implementation of the European Geological data Infrastructure (EGDI). These relate e.g. to the following aspects: identity management and digital credentials, electronic signatures, the risks and opportunities of cloud computing, data protection and security, digital rights management and access control. It should be kept in mind that trust may also relate to the concept of legitimate expectations and good governance, hence it may also have an impact on the governance model that will be presented in one of the next deliverables in this project.

No matter how the EGDI is designed, its most important aspect is that it can and will be used by all organisations and people needing geological data. For this to be materialised, it is essential that the EGDI invokes sufficient trust from both the providers and users in that they are certain that their rights and interests are being safeguarded, that they can count on the data, services, technology, policies and people that are part of the infrastructure. In

[1] F. Sultan et al. (2002). "Determinants and Role of Trust in E-business. A Large Scale Empirical Study", *MIT Sloan School of Management Working Paper*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=380404 (accessed on 22/05/2013).

[2] J. Dumortier et al. (2011). "D.7.1 Legal Requirements for Trust in the IoT", *uTRUSTit project report*, http://www.utrustit.eu/uploads/media/utrustit/uTRUSTit_D7.1_Legal_Requirements_for_Trust_in_the_IoT_final.pdf (accessed on 22/05/2013). (hereafter: [Dumortier et al 2011.])

[3] E.g. relating to the legal entity 'trust', used for charities or family estates.

[4] M. Cohen (1933). "The Basis of Contract", *Harvard Law Review* 46(4), 578-580; C. Caufmann (2005). *De verbindende eenzijdige belofte*. Antwerpen: Intersentia, 952 p.

general, one could say that three main domains can be envisioned in which a relationship of trust needs to be developed: trust in the data, trust in the services, and trust in the people.

Trust in the data

For the user to feel comfortable in using the geological data sets (both primary and derived) offered by the EGDI, he or she has to have enough guarantees and safeguards that the data are reliable and of sufficient quality and fitness for purpose for the objectives he wants to obtain. Several measures and tools are available to increase this trust, including metadata, transparent quality assessment procedures, authoritative data, security measures for maintaining the authenticity and integrity of the data, etc. The more different providers of data are included in the EGDI, the more difficult it will be to maintain the trust in the data.

Trust in the services

If a user has to rely on obtaining data via services such as the INSPIRE network services, he or she has to be able to rely on the availability of these services whenever they are needed. Hence, a sufficient level of service has to be guaranteed by the service providers in the EGDI, and the offered level of service has to be communicated clearly to the users of the services via what is generally referred to as service level agreements or terms of service. The required level of service is to a large extent determined by the INSPIRE implementing rules relating to the network services, but may also need to be laid down for other services in the EGDI.

Trust in the people

An essential part of the EGDI is the people and organisations that are using it, both to provide data and services and to use these data and services. For the data providers it may be important, depending on the data and use conditions, to know who is using their data and how they are using it. For the data users it is important to know who the data is stemming from and that access and use of the data is not unnecessarily restricted. In addition, they need to be sure that the information on their identity and their use of the data is not misused by the data provider. This relationship involves issues such as authentication and identity management, rights management and personal data protection.

Trust in the EGDI may have different levels and different forms. For instance, in the case of open data, trust will mostly involve the guarantee to the users that the data will remain openly available in the future, but it may also refer to the trust users can put in the accuracy and currency of the data, as outlined in the metadata. In case of restricted data, trust will be more linked with the security and confidentiality of the data and services: how can it be safeguarded that only the persons who are authorised to see or use the data, are able to do so?

The measures that are necessary to develop trust may also differ according to the technology that is used. One of the options for the EGDI would be not to develop a separate infrastructure, but rely on existing infrastructure offered by the private sector, i.e. the cloud. This may have an impact on the way the EGDI needs to be organised and what measures are sufficient for ensuring trust.

In the following sections, we will give an overview of the main elements in the European regulatory and policy framework that need to be taken into account in the creation of a trusted EGDI. These elements will in most cases require a particular decision or the development of a process by the governance structure that will be built to develop and maintain the EGDI. This report does not aim to provide these decisions or processes, but only to highlight that they need to be made.

2 Elements of trust in the EGDI

As already indicated in the introduction, ensuring trust in the EGDI involves on the one hand the promotion of transparency and openness about the data and services that are being offered; and on the other hand security measures that protect the confidentiality of data and services if needed. A proper balance needs to be sought between both aspects, taking into account the required accessibility of the data and services.

For instance, if the EGDI chooses in its first stage to focus on open data, it may not require much attention for security measures. However, it can be assumed that not all data will be openly available and that access to some data and services will be restricted to authorised persons, for instance for national security reasons. In such cases, security measures to protect the integrity and authenticity of the data and access control mechanisms will be required. Making the EGDI into a trusted infrastructure involves applying the measures when necessary, based on an impact assessment and with an eye for the proportionality of the measures.

2.1 Trust in the data

Trust in the data included in the EGDI relates to a number of aspects: integrity, authenticity, but also the quality of the data. However, quality can have different meanings. For some, it relates to the consistency with specifications, while for others it is about meeting or exceeding their expectations, in the context of the use they want to make of the data.[5] Therefore to establish trust in the quality, it is essential that information is given about the quality of the data. Next, the quality of the data needs to be protected, in that safeguards are built in that the data are not tampered with, and that their integrity and authenticity can be guaranteed.

2.1.1 Metadata

A first tool to increase trust in the geological data that is included in the EGDI, is the availability of high-quality metadata for all data sets and services. Metadata is ‘data about data’, informing the users about the creator of the data, its purpose, scale, quality, actuality and accuracy, etc, or the characteristics of the service. Metadata enables the users to find the most appropriate data sets or services to fit their requirements.[6] Hence, users will base their decisions on the information they get in the metadata.

[5] R. Devillers et al. (2002). “Spatial Data Quality: From Metadata to Quality Indicators and Contextual End-User Manual”, *OEEPE/ISPRS Joint Workshop on Spatial Data Quality Management*, 45-55, http://www.researchgate.net/publication/228597904_Spatial_data_quality_From_metadata_to_quality_indicators_and_contextual_end-user_manual/file/d912f50b7c95e4c6c2.pdf. (hereafter [Devillers et al. 2002])

[6] A. Rajabifard et al. (2009). “SDI and Metadata Entry and Updating Tools” in B. Van Loenen et al. (ed.). *SDI Convergence. Research, Emerging Trends, and Critical Assessment*, Delft: Netherlands Geodetic Commission, 121-136.

Therefore, these metadata have to contain sufficient and correct information on the data or service they refer to. Geological data falling under the field of application of the INSPIRE directive have to be accompanied by the following metadata (article 5 INSPIRE directive[7]):

- the conformity of spatial data sets with the Commission Regulation implementing the INSPIRE directive as regards metadata[8];
- conditions applying to access to, and use of, spatial data sets and services and, where applicable, corresponding fees;
- the quality and validity of spatial data sets;
- the public authorities responsible for the establishment, management, maintenance and distribution of spatial data sets and services;
- limitations on public access and the reasons for such limitations, in accordance with Article 13 of the INSPIRE directive.

The Commission Regulation on metadata of 3 December 2008 contains the specific metadata elements that have to be included and specific instructions on how to describe these metadata-elements. While these requirements would not be applicable to geological data that does not fall under the field of application of INSPIRE, it deserves recommendation to streamline the metadata process as much as possible and to include the same metadata elements in their description.

Metadata are an important element to create accountability and to assign liability in case of potential damages occurring due to or in the course of the use of the data. With regard to liability, an important part of the metadata is the statement of what the data are not.[9] It can be used to clarify the purpose for which the data was collected, and the purposes for which it is suitable to be used, and particularly also not to be used. Moreover, it can contain references to statements limiting liability and imposing possible use constraints. Ideally, metadata should contain warnings and cautions with regard to the expected use, inform the user on the product risk and dangers and the means to take precautions against these risks.[10] However, this is not always possible. It depends on the national liability regimes in how far metadata can provide sufficient information about the data to avoid liability.

2.1.2 Quality assessment and assurance procedures

While the availability of metadata may make the user aware of quality issues with a particular data set, he or she may not have at his disposal any tools to fully assess the quality of the dataset, or any means for quality assurance.[11] Quality is defined by ISO 8402 as the

[7] European Parliament and Council (2007). Directive 2007/2/EC of of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), *OJ L* 108, 25 April 2007, 1-14.

[8] European Commission (2008). Regulation 1205/2008 of 3 December 2008 implementing Directive 2007/2/EC of the European Parliament and of the Council as regards metadata, *OJ L* 326, 4 December 2008, 12.

[9] L. Wayne (2005). “Metadata in Action. Expanding the Utility of Geospatial Metadata*”, GIS Planet* June 2005, 1-6,

[10] [Devillers et al. 2002]

[11] D. Li et et al. (2012). “Spatial data quality and beyond”, *International Journal of Geographic Information Science*, 26(12), 2277-2290. (hereafter [Li et al. 2012])

"totality of characteristics of a product that bear on its ability to satisfy stated or implied needs". Hence, to define quality both the information on the data that is being used and on the user needs are required.[12] Current metadata have strong limitations for communicating this quality.[13] For instance, they often do not contain warnings or directions with regard to the expected use of the data.[14] In addition, the information provided by metadata is not easily accessible for non-expert users.[15] Research has shown that metadata often did not play a significant role in data consumers' perception of the data, but that they used other ways to establish an opinion about the data quality.[16]

Enabling full quality assessment and assurance entails not only knowing the information in the metadata, but also more information about the legacy of the data, the collection and validation process, etc. This allows the user to make a risk assessment relating to the fitness for purpose of the data.[17] In addition, it may also provide increased protection for the data provider against possible liability claims.

If such information is available about the legacy and collection process of the data, and particularly how the quality of the data is checked and valued, making this information public could increase the trust in the EGDI and its data. However, incomplete or unclear information may actually decrease the trust in the EGDI, so the data providers will have to assess carefully whether it could be useful to make more information available about the data beyond what is already part of the metadata. The development of a standard quality description method could remedy this.[18]

2.1.3 Authoritative data or authentic sources

While the term authoritative data can have a number of meanings and it is sometimes just referring to the fact that the data stems from a public body responsible for the collection of that data, the term sometimes also refers to authentic sources. For such authentic sources, the quality is assumed: they are considered to be accurate and reliable so that they can or usually even *should* be used in official procedures, e.g. for evidentiary purposes. The concept of authentic sources is related to one of the basic principles of INSPIRE: collect the data once at the most suitable place, and re-use the data multiple times. Authentic sources are generally recognised by law, and have to comply with stringent quality requirements.[19]

[12] [Devillers et al. 2002].

[13] [Devillers et al. 2002].

[14] [Devillers et al. 2002].

[15] R. Devillers et al. (2007). "Towards Spatial Data Quality Information Analysis Tools for Experts Assessing the Fitness for Use of Spatial Data", *International Journal of Geographical Information Science*, 21(3), 261-282. (hereafter [Devillers et al. 2007])

[16] A. Boin and G. Hunter (2007). "What Communicates Quality to the Spatial Data Consumer?", *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences* 34 (XXX), http://itc.nl/external/ISSDQ2007/proceedings/Session%205%20Dissemination%20and%20Fitness%20for%20Use/Boin_paper%5B1%5D.pdf (accessed on 22/05/2013).

[17] [Li et al. 2012].

[18] An attempt for such a method has for instance been made by [Devillers et al. 2007]. Inspiration can of course also be found in literature relating to data and information quality outside of the spatial sector.

[19] See e.g. http://www.corve.be/english/authentic-sources/index.php.

It may be the case that particular national data sets that will be included in the EGDI have already been adopted at the national level as authentic sources through a legally prescribed procedure. In order to increase the trust in the EGDI, it could be considered to set up 'pan-European authentic sources' next to or on the basis of these national data sets.

If this would be considered, then as a consequence appropriate procedures need to be set up to determine the requirements for such data regarding to quality, accuracy, currency and validation of the data; the security requirements relating to the integrity and authenticity of the data; and the entity responsible for maintaining the data. The use of such authoritative sources would benefit interoperability in the EGDI. However, if the national requirements are very different, the development of a 'pan-European' authentic source may be very complicated.

2.1.4 Security of the data in the EGDI

In the development of the EGDI, security will take an important place. Security can be defined as the countermeasures, or controls, employed to protect the availability, access, confidentiality, integrity and authenticity of an information system or infrastructure.[20] As a starting point, it should be kept in mind that there is no such thing as absolute security. As Cronin states, "the only way to protect a computer from Internet threats is to unplug it, both from a telecommunication connection and from the wall".[21]

While there are few legal provisions relating to security in general, legal obligations exist with regard to e.g. the protection of personal data, the protection of financial data, authentic sources, etc. However, many of these obligations can easily be transposed as good practices for ensuring security for all types of data in an infrastructure such as the EGDI. In setting up the infrastructure, the entities involved in the EGDI will have to assess what levels of security are needed for the data included in the EGDI, and how to implement these possible different security levels. For instance, in the case of open data, security requirements can be limited in the sense that there is no need to limit access to particular persons. However, the data providers may still wish to ensure the integrity of the data for liability reasons.

Three types of security measures can be distinguished: technical measures, physical measures and administrative measures.[22] The first type of measures involves safeguards incorporated into hardware, software and related devices. Physical security measures protect tangible items such as the actual computers from destruction. Administrative measures are procedural management controls and policies. For each of these categories, there are measures for prevention, detection and reaction.[23]

[20] J. Soma et al. (2011). "Chasing the clouds without getting drenched: a call for fair practices in cloud computing services", Journal of Technology Law & Policy 16, 193-227 (hereafter [Soma et al. 2011]); K. Cronin (2010). "Best practices and the state of information security", *Chicago-Kent Law Review* 84, 811-819 (hereafter [Cronin 2010]).

[21] [Cronin 2010].

[22] [Cronin 2010].

[23] [Cronin 2010].

In its Guidelines for the Security of Information Systems and Networks, the OECD has set out nine principles that should underpin any discussion about a security policy in a network, system or infrastructure such as the EGDI. These principles include:[24]

1. Awareness: Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2. Responsibility: All participants are responsible for the security of information systems and networks. Each participant should understand its own responsibilities.
3. Response: Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
4. Ethics: Participants should respect the legitimate interests of others.
5. Democracy: The security of information systems and networks should be compatible with essential values of a democratic society.
6. Risk Assessment: Participants should conduct risk assessments.
7. Security design and implementation: Participants should incorporate security as an essential element of information systems and networks. Both technical and non-technical safeguards should be considered, proportionate to the value of the information included in the systems and networks.
8. Security management: Participants should adopt a comprehensive approach to security management. This approach should include all levels of participants' activities and all aspects of their operations. It should address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit.
9. Reassessment: Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

Of course, whatever security measures are imposed, they have to be weighed against the need for user-friendliness of the applications included in the EGDI. To prevent users from refraining from using the data and services offered by the EGDI because of difficult or demanding security procedures, the security measures should require minimal user effort and ideally run mainly on the background without requiring active user input.[25]

2.1.4.1 Protection of data availability

An important part of security includes the protection of the data against accidental or wilful destruction or loss. This is mostly relevant for the availability of data. This availability does not only entail that the data has to be on a storage device that is physically intact and undamaged, but also that it can be accessed by a computer with software capable of reading and interpreting the data in order to display it in a digital form.[26] Hence, the information and

[24] OECD (2002). *Guidelines for the security of information systems and networks: towards a culture of security*, http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm (accessed on 24/05/2013).

[25] [Dumortier et al. 2011].

[26] T. Smedinghoff (2007). "It's all about trust: the expanding scope of security obligations in global privacy and e-transactions law", *Michigan State Journal of International Law* 16(1), 1-47,

the system must be sufficiently robust to withstand external events, such as power failures, natural disasters or attacks, but also issues such as media deterioration and obsolete formats have to be taken into account.[27]

2.1.4.2 Protection of data integrity and authenticity

The authenticity of a document refers to the fact that it can be established that the document emanates from the source that it claims. Data integrity deals with the accuracy and completeness of information, and with ensuring that no unauthorised alterations are made to the data, whether intentionally or not.[28] This is particularly important in the case of authoritative data or authentic sources. Documents that are not protected can be altered easily and in a manner that is not detectable. In addition, as every copy of an electronic record is a perfect reproduction, there is no such thing as an original electronic record. So there are no assurances about the status of the content of an electronic record.[29] Therefore, data origin authentication protocols should be set up.[30]

However, there are few established means to ensure the authenticity and integrity of electronic information. One of the methods that can be used, is the use of logs or audit trails. Such audit trails can provide a complete log of all transactions relating to specific information performed by users or systems. They can be used to trace the origins and whereabouts of information, and any changes that are made to the date, e.g. in the form of updates or corrections. As such this provides proof of the authenticity and integrity of a document and increases trust.[31] Traceability is also important for determining accountability and liability. It is not sufficient to know that changes have been made, but it needs to be checked whether these changes were made by authorised persons. This requires authentication and authorisation mechanisms, which will be discussed later in the section on identity management.

Another means to ensure the integrity and authenticity of a document, in this case a data set, is the use of electronic signatures. This is supported by a European legal framework in the form of the European Directive on a Community framework for electronic signatures (E-signature Directive).[32] This directive and the concept of electronic signatures will be discussed further on in the report, in the chapter on trust in people. As an electronic signature only provides for integrity at the level of the bitstream, not the level of the document itself,

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1100712 (accessed on 23/05/2013). (hereafter [Smedinghoff 2007])

[27] [Smedinghoff 2007].

[28] [Smedinghoff 2007].

[29] [Smedinghoff 2007].

[30] B. Van Alsenoy et al. (2011). "D3.1. Legal Provisions for Deploying INDI services", *GINI Support Action project report*, http://www.gini-sa.eu/images/stories/2011.11.06_GINI_D3.1_Legal%20Provisions%20for%20Deploying%20INDI%20Services_FINAL.pdf (accessed on 22/05/2013). (hereafter [Van Alsenoy et al. 2011])

[31] [Dumortier et al. 2011].

[32] European Parliament and Council (1999). Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures (E-signature Directive), *OJ L* 13, 12-20.

this is not really useful.[33] E.g. a single change in a bit of a file could damage the integrity of the bitstream, while it may actually not have altered the document contained in the file at all.

2.1.4.3 Protection of confidentiality

Another objective of security is to ensure the confidentiality of information, i.e. keeping the content of the information secret from all entities except those that are authorised to see it.[34] There are several ways to ensure this confidentiality, including physical security (making sure only authorised persons can access a building or a room), access control and cryptography. In case the EGDI decides that it needs to organise such measures to ensure confidentiality of particular data sets, it should not only clearly delineate who can be granted access to particular data or services, but also how far these access rights go.[35] This may result in dividing possible users of the data and services included in the EGDI in different groups or categories and assigning particular roles to each of these groups. This topic will be addressed further in the chapter on trust in people.

A particular type of data requiring confidentiality is personal data. As the data sets included in the EGDI will almost never be qualified as personal data, this topic is not dealt with in this section. The only personal data that will be processed will most likely be the data regarding the persons accessing the data and services in case of restricted data. Therefore, the processing of personal data is discussed in the chapter on trust in people in the section on identity management.

2.1.5 Impact on the EGDI

There are a number of questions that need to be considered in the roll-out of the EGDI with regard to trust in the data. For a number of these questions, it could be stated that these issues form the technical counterpart of the governance structure that needs to be set up, which will be discussed in D9.3. Issues that need to be considered include:

- Metadata: for data sets that fall under the scope of INSPIRE, the metadata requirements are made clear in the INSPIRE implementing rules. It is recommended that for the other data sets included in the EGDI, it is examined in how far the metadata requirements of INSPIRE can also be applied. Next, it should be examined in how far the metadata can include information on the fitness for purpose.
- Quality information: the data providers in the EGDI should consider whether it would be useful and feasible to design a standard method for the description of quality of the geological data included in the EGDI.
- Authentic sources: the EGDI data providers should consider how they will deal with national authentic sources. If they choose to create pan-European authentic

[33] [Dumortier et al. 2011].

[34] [Van Alsenoy et al. 2011].

[35] [Dumortier et al. 2011]; D. Steinauer et al. (1997). "Trust and traceability in electronic commerce", *StandardView* 5(3), 118-124. (hereafter [Steinauer et al. 1997])

sources, a process should be developed for the creation and recognition of these sources.

- Security: the EGDI data and service providers should set up a security policy that provides sufficient security, but also maintains as much user-friendliness as possible. Such a security policy includes an assignment of responsibilities, including decisions on the entities responsible for developing and updating the security policy, maintaining logs for operations, serving as a point of contact for security breaches, performing the compliance audits, etc.

2.2 Trust in the services

With regard to establishing trust in the services, the EGDI service providers will also have to make sure that transparency and security requirements are complied with. An additional element to include in the EGDI for services, are service level agreements. Moreover, digital rights management technology will be important. Such technology is also very relevant in the next section on trust in the people, and shows that data security, DRM, access management, and identity management are all elements of an encompassing security framework that needs to underpin the EGDI.

2.2.1 Metadata and quality information

Services in the EGDI falling under the scope of the INSPIRE directive will also need to be described in metadata according to the INSPIRE implementing rules. Here it can also be recommended that for other services, it is assessed whether the metadata requirements for INSPIRE can also be applied.

While the fitness for purpose may be easier to discover for the users of the services, it should also be examined in how far more information about the quality of the service can be provided. This information will in many cases take the form of a commitment of the service provider in a service level agreement.

2.2.2 Service level agreements

In order for the EGDI-services to be used, their performance will have to be sufficient for users to be able to rely on their availability at the moment they need them. Therefore, the users have an interest in the service level agreements or service level guarantees that are offered by the EGDI service providers.

In the case of INSPIRE network services, a minimum level of service is imposed by the INSPIRE implementing rules. However, for any other service the EGDI intends to offer, the entity responsible will have to consider which level of service it can/is willing to give, and lay this down in its service level agreements or terms of service, in order to inform the users and to determine its level of commitments and, consequently, its level of liability in case of non-performance.

Effective SLAs that are useful for both parties often consist of at least the following five elements: 1) metrics focused on key performance indicators; 2) reasonable remedies for failure to achieve targeted performance levels; 3) the ability of the service provider to gain back any monetary remedies through enhanced performance; 4) a method to determine and remedy the cause of the failure; and 5) a process for periodic review and adjustment of the SLAs.[36] In designing the performance metrics, the focus has to be on what is useful, at the same time taking into account what can reasonably be measured.

Monitoring of the use of the services will be important for maintaining the service level agreement, or to allow for an increase in capacity in case there is a need, for example in the case of an emergency requiring immediate access to very large amounts of data, or in case of the launch of a new service attracting attention from a very large audience. Such monitoring is generally considered part of so-called digital rights management.[37]

As the EGDI wants to offer pan-European services, it will have to be examined which service level can be offered or such services, and in how far the minimum service level can be harmonised between the different service providers involved in the EGDI.

2.2.3 Security

The security policy that is developed for the data included in the EGDI should be extended to the services. With regard to the services, it is important that the continuity can be guaranteed, in the sense that the services are protected against attacks (e.g. denial of service attacks), network outages and other external events. Access management will also be essential in this perspective: ensuring that only authorised persons have access to the service, and only use the data for the purpose for which they have an authorisation. This will be discussed in the chapter on trust in people. This access management is also closely related to digital rights management.

2.2.4 Digital rights management

In the EGDI, the data providers will be confronted with the challenge of controlling the dissemination of their data and services downstream in the geospatial value chain[38] (assuming that they want to track the use of their data, which will be the case for restricted data, but actually also may be the case for 'open' data).

Bishr et al. state that two definitions of DRM exist: a narrow one and a broad one. The narrow definition focuses on protection of digital content, in that it allows the distributor of the content to control how the data is used, and by whom. The broad definition of DRM includes everything that is required to define, manage, and track rights on digital content. In addition to protection, this also includes business rights or content rights and access tracking.[39] The EGDI will have to consider how to implement DRM in this broad definition. The main focus of such implementation should be on the management of rights, rather than the

[36] M. Dunne (2008). "Eight significant points in technology outsourcing and remote hosting contracts", *New Jersey Lawyer* 255, 19-22.

[37] Cf. infra.

[38] M. Bishr et al. (2007). "GeoDRM: Towards digital management of intellectual property rights for spatial data infrastructures" in H. Onsrud (ed.), *Research and Theory in Advancing Spatial Data Infrastructure Concepts*, Redlands: ESRI, 245-260. (hereafter [Bishr et al. 2007])

[39] [Bishr et al. 2007].

protection. The EGDI can make use of the GeoRM framework, developed by the Open Geospatial Consortium (OGC).[40]

GeoRM was specifically developed for geospatial data by the OGC. It can be described as "a set of technologies and legal frameworks that are fit for a certain organisational need, enabling rights-managed geospatial networks, such as SDIs, where all rights over geospatial assets are specified by licensors and any licence would be trusted to honour the licensor's conditions within and beyond the network's trusted environment".[41] Hence, GeoRM is not just about technology, or just about licensing: the combination of both should enable the mapping of licensing policies to digital assets and the management and tracking of the use of these digital assets.[42]

The GeoRM Reference Model's purpose is to create a simplified model of intellectual property rights for geospatial data so that it can be practically licensed, managed and protected.[43] The model accommodates licensing for different types of business relationships and participants with different roles, including direct licensing, indirect licensing, B2B, and B2C. It also enables licensing for dynamically created geographic information by using Web Mapping Services (WMS) and Web Feature Services (WFS).[44] In order for this to work, there may be a number of necessary modules: of course the rights model and the rights expression language[45], but also encryption, licence verification, authentication, authorisation, and enforcement.[46]

2.2.5 Impact on the EGDI

Also with regard to the services included in the EGDI, a number of decisions will have to be made, and policies developed. Points of attention for the EGDI governance structure include the following.

- Metadata and quality information: for the EGDI services that fall under the field of application of INSPIRE, the metadata requirements are made clear in the INSPIRE implementing rules. It is recommended that for the other services included in the EGDI, it is examined in how far the metadata requirements of INSPIRE can also be applied. Next, it should be examined in how far the metadata can include information on the fitness for purpose, and which other channels can be used for providing information on the characteristics of the services.
- Security: the security policy that needs to be developed by the data and service providers in the EGDI needs to pay sufficient attention to services, particularly with

[40] See http://www.opengeospatial.org/.
[41] [Bishr et al. 2007].
[42] [Bishr et al. 2007]; L. Aslesen et al. (2010). "D4.4. Best practice for a licensing policy (including pricing and geo rights management)", *ESDIN project report*, http://www.esdin.eu/sites/esdin.eu/files/D%204.4%20Final%20Licensing%20policy%20guidelines.pdf (accessed on 23/05/2013).
[43] See http://churchilledemba.blogspot.be/2012/12/geospatial-digital-rights-management.html.
[44] See http://churchilledemba.blogspot.be/2012/12/geospatial-digital-rights-management.html.
[45] GeoREL (Geographic Rights Expression Language), is an XML language to describe access rights. It has been adopted as an ISO standard.
[46] See http://churchilledemba.blogspot.be/2012/12/geospatial-digital-rights-management.html.

regard to access management and guarantees for continuity. In developing this security policy, the role of each party in the EGDI governance structure needs to be clarified. Will the security policy be centrally organised? Will there be coordination between the data and service providers? Who will be responsible for maintenance, etc?

- Service level agreements: the INSPIRE implementing rules already contain particular service level requirements for the services that fall under the INSPIRE directive. For the other services, service level agreements or terms of service will have to be developed that are feasible for the service providers and that at the same time are sufficient for the users of the EGDI. The EGDI governance structure should consider whether it wants to propose common service levels for all or particular categories of services in the infrastructure.

- Digital rights management: it should be considered to what extent rights management technology is required and what its exact function should be. Any such technology should be implemented in coordination with the licensing policy that is set up in the EGDI. The GeoRM and GeoREL standards should be used. Some data and service providers in the EGDI may not be ready to implement rights management technology. The readiness of these organisations should be measured and a support and implementation strategy should be rolled out.

2.3 Trust in the people

While many data in the EGDI may be open, this will most likely not be the case for all data or services included in the infrastructure. Therefore, the EGDI will have to include processes for assessing which data and services should possibly not be open, but to which access should be restricted. After these data and services have been selected, a second process should be set up to determine which people should get access to these data and services, i.e. which levels of restrictions need to be built in, which roles and profiles should be set up for access, and which procedures should be created for making sure that only authorised people access the data or services. Generally, the latter types of procedures are referred to as identity and/or access management. As mentioned before, such management is also important for the trust in the other elements of the infrastructure, i.e. the data and services.

The main challenge for the EGDI will be implementing identity and access management for cross-border services and applications. Federated identity management will probably be the most suitable solution for arranging this. The new initiative of the European Commission with regard to the mutual recognition of national credentials should also be followed up.[47]

Incorporating identity management in the EGDI will entail the processing of personal data of the people accessing the data and services. In order to ensure the trust of the users in the infrastructure, it is essential that these personal data are treated in full compliance with the rules and principles of the European legislation on personal data protection. In this sec-

[47] Cf. infra.

tion, we will give an overview of the main obligations of the controller of the persona data processing operations. But first, we highlight some of the main aspects of identity management.

2.3.1 Identity management

The process of identity management involves a number of different steps that need to be taken for the provision of data and services in the EGDI. However, before this process is started, it needs to be determined for each dataset and service, whether and in how far such identity management is necessary. For instance, if a data set is available as open data, there will be no need to set up authentication and authorisation procedures, because anyone can use the data freely for any purpose he chooses. For service management reasons, the provider may choose to offer 'almost open data' and implement a minimal level of access management. For data or services that need to be strictly restricted to authorised persons, a stronger identity management process will need to be implemented.

The following steps make up the identity management process. First, users need to be registered in order to assign them their specific roles and credentials for giving them access to certain (categories of) data or services. Second, the users need to identify themselves, for instance by providing their real name, user name, or an identification number. Third, the user is authenticated, verifying whether he or she is who he claims to be and belongs to the organisation he or she claims. The authentication of a person entails "the presentation of authentication information that confirms the association between a person and an identifier". In short, authentication provides a level of assurance as to whether someone is who he or she claims to be.[48] This information can be something the person knows (a password, PIN code), possesses (a token, smartcard, passport) or is (biometric data).[49] Once a person's identity is authenticated, the business relying on that authentication will determine what rights and privileges are accorded to that person, i.e. authorize his or her access.[50] In computer systems and networks, this final process is often referred to as access control.[51]

After identification and authentication, such access control mechanisms are needed to enforce the rules, for instance based on Role Based Access Control technology. This technology allows access to functions or data based on the role that is defined for an individual in a given context, and not just by his identity.[52] Hence, this can control the attributes assigned to the person, e.g. staff member of a particular department in an organisation, allowed to use a dataset or service.

[48] [Smedinghoff 2007].

[49] E. Mik (2012). "Mistaken identity, identity theft and problems of remote authentication in e-commerce", *Computer Law & Security Review* 28(4), 396-402. (hereafter [Mik 2012])

[50] T. Smedinghoff (2009). "Federated Identity Management: Balancing Privacy Rights, Liability Risks, and the Duty to Authenticate", http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471599 (accessed on 23/05/2013). (hereafter [Smedinghoff 2009])

[51] [Smedinghoff 2009].

[52] [Steinauer et al. 1997].

2.3.2 Identity management in cross-border transactions

One of the main problems that the EGDI will face in relation to the organisation of authentication and authorisation processes is the cross-border use of electronic identities and identifiers. There is currently no encompassing framework for the mutual recognition of electronic credentials for accessing government or private services. The only legal framework that exists is the 1999 European Directive on electronic signatures (E-signature Directive).[53]

The E-signature Directive puts in place a system for the mutual recognition of qualified digital signatures.[54] However, beyond this system of qualified certificates, there is no general assurance mechanism for recognition (and the liability linked to this recognition) between countries.[55] In the absence of such a generally recognised mechanism, the EGDI will have to consider how to organise the cross-border access to data and services in such a way that the user can obtain seamless and direct access to all data and services. It will have to assess what type of authentication mechanisms are appropriate for each application,[56] and determine how such a mechanism will be rolled out across the entire EGDI.

In determining this, the EGDI may have to take into account the existence of various national systems, with different methods and security levels for authentication. For instance, some organisations may assure someone’s identity by asking them to reply to an e-mail, while others will ask them to come to the entity’s offices personally. Next, some may deliver their own set of identity credentials, such as passwords, while others may rely on credentials provided by third parties, such as a national token.[57]

This also implies the allocation of liability in case of breach, i.e. in case data or services are accessed by unauthorised persons or used by authorised persons for purposes beyond their authorisation level. This is linked to the level of enforcement that is envisaged: will each data or service provider in the EGDI take care of the validation, will this be assigned to one entity within the EGDI, or will an external certification authority be involved[58]?

[53] European Parliament and Council (1999). *Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures (E-signature Directive)*, *OJ L* 13, 19 January 2000, 12-20.

[54] For more information on digital signatures, see e.g. [Mik 2012]; [Van Alsenoy et al. 2011]; J. Dumortier and N. Vandezande (2012). “Trust in the proposed EU regulation on trust services?”, *Computer Law & Security Review* 28(5), 568-576 (hereafter [Dumortier and Vandezande 2012]); C. Spyrelli (2002). “Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication”, *Journal of Information Law and Technology* 2(2), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/?textOnly=false (accessed on 23/05/2013).

[55] [Van Alsenoy et al. 2011].

[56] [Van Alsenoy et al. 2011].

[57] ENISA (2011). *Mapping security services to authentication levels. Reflecting on STORK QAA levels*, http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/map-auth-lev/at_download/fullReport (accessed on 22/05/2013). (hereafter [ENISA 2011])

[58] Cf. infra.

2.3.3 The E-signatures directive

The E-signature Directive establishes a legal framework for electronic signatures and certain certification services.[59] Its objective is to facilitate the use of electronic signatures and to contribute to their legal recognition in the internal market. Under the directive, there are three types of electronic signatures[60]:

- Ordinary electronic signatures: any data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication[61];
- Advanced electronic signatures: electronic signatures that meet the following requirements:
  - They are uniquely linked to the signatory;
  - They are capable of identifying the signatory;
  - They are created using means that the signatory can maintain under their sole control; and
  - They are linked to the data to which they relate in such a manner that any subsequent change in the data is detectable.
- Qualified electronic signatures: advanced electronic signature that are
  - Based on a qualified certificate provided by a certification service provider who fulfils the requirements laid down in the annexes of the E-signatures Directive;
  - Creating using a secure signature-creation device (meeting the requirements in the annexes of the E-signatures directive).

The difference between the types of signature lies in the legal recognition of the signature as equivalent to a handwritten signature on a paper document.[62] Under article 5.1 of the E-signature Directive, a qualified electronic signature must be given the same legal effect as a handwritten signature. If the requirements for the qualified character of the digital signature are not fulfilled, this does not mean that the signature should not be given legal effect, but that such legal effect can be denied if the technology behind the signature is not considered adequately reliable. Denial of legal effect of the signature cannot be merely because it is in electronic form, not based upon a qualified certificate, not based upon a qualified certificate from an accredited certification-service provider or not created by a secure signature-creation device[63] Hence, the validity of the signature cannot be denied merely because it is electronic, but there need to be additional technical reasons. If the signature is a qualified one, the validity cannot be denied at all.

In practice, the system of qualified electronic signatures is hardly used. The reason for this is twofold. First, people do not use the solution because it is not readily available when they need it, because it has not been widely adopted by market players. Second, in many situa-

[59] [Van Alsenoy et al. 2011].

[60] [Van Alsenoy et al. 2011].

[61] Art. 2.1 E-signature Directive.

[62] [Van Alsenoy et al. 2011].

[63] Art. 5.2. E-signature Directive.

tions, people do not need a qualified electronic signature, and other trust mechanisms are preferred.[64]

2.3.4 Revision of the E-signatures directive

Under the Digital Agenda for Europe, the European Commission proposed a revision of the E-signature Directive.[65] The objective of the draft Regulation "on electronic identification and trust services for electronic transactions in the internal market" is to provide a legal framework for cross-border recognition and interoperability of secure e-authentication systems.[66] The regulation will cover two topics: electronic identification and trust services. The cross-border authentication in the context of online public services will be addressed by a specific Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online authentication mechanisms offered in all Member States.[67]

The proposed Regulation determines in its Article 5 that wherever authentication is required – either by legislation or by administrative practice – to access an online service, this service should also be accessible for people using electronic identification means (such as e-ID cards or tokens) issued in other Member States, provided that these identification means are included in a list published by the European Commission.[68]

This mutual recognition scheme is based on the work done in the STORK project, which aimed at making the cross-border operation of online public services easier for citizens.[69] Particularly the pilot on the use of government portals from different EU Member States, which can be accessed with credentials from any of the other participating Member States, is interesting for the deployment of the EGDI.

Under the draft Regulation, it is not exactly clear how this mutual recognition scheme should work. For instance, Article 5 does not take into account the possible differences in security levels. The list of identification means provided by the Commission will contain all kinds of security levels: from simple passwords to highly secured e-ID cards.[70] At the moment, the regulation does not seem to require matching or equivalent security levels for the cross-border authentication. However, it seems logical that online public services requiring strong authentication in one Member State will not be accessible by using a simple password scheme from another Member State. It will be important to follow up how this issue is dealt with in the final version of the Regulation. In addition, also important for the EGDI, the Regulation only addresses the authentication of the identity of the person, and not the pos-

[64] [Dumortier and Vandezande 2012].

[65] European Commission (2010). *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A digital agenda for Europe*, COM (2010) 245 final.

[66] European Commission (2012). *Commission proposal for a regulation of the European Parliament and of the Council of 4 June 2012 on electronic identification and trust services for electronic transactions in the internal market*, COM(2012) 238 final. (hereafter [European Commission 2012]).

[67] [Van Alsenoy et al. 2011].

[68] [European Commission 2012].

[69] See https://www.eid-stork.eu/.

[70] [Dumortier and Vandezande 2012].

sible attributes, such as whether this person is qualified to represent his organisation (e.g. is he or she actually a civil servant working for the public authority that has access to particular restricted data?).

Another criticism of the cross-border recognition introduced by the draft Regulation is that it would include all online public services, including services that are inherently local or have a limited geographic reach, e.g. local libraries. As the EGDI is specifically targeting cross-border use of geological data and services, the recognition scheme will be relevant. However, when more local data and services are added, the impact of the regulation may be higher than desired. Of course, the final text of the Regulation will have to be awaited to determine this.

The second part of the proposed Regulation deals with trust services, which are defined as "any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signatures and for electronic seals".[71] The use of electronic seals may be important for the EGDI in case the data provider needs to prove the origin and integrity of a document that does not require a signature; and electronic time stamping may be important in cases where it is essential that the date a particular data set was created, updated and/or validated can be proven beyond any doubt. It needs be examined whether the use of electronic seals and/or time stamps may become necessary in the EGDI.

The further development of the draft Regulation and the specific Decision on identification and authentication will have to be followed up in the course of EGDI-scope and the further development of the EGDI.

2.3.5 Federated identity management

In order to enable chained services and to facilitate the use of cross-border data and services, the EGDI should consider how to implement federated identity management, and work with a so-called 'single sign-on' for the services in the infrastructure. Federated identity management allows businesses or governments to outsource the identification and authentication processes to a third party, and eases the burden on users and consumers by allowing them to use a single sign-on for multiple services, rather than having to track numerous user-IDs and passwords.[72]

For the businesses or government agencies involved, this means that they don't have to handle the difficult and expensive task of identity management and that they can leverage the identification and authentication done by others.[73] Federated identity technology allows

[71] [European Commission 2012].

[72] [Smedinghoff 2009].

[73] [Smedinghoff 2009].

organisations using disparate authentication and authorisation methods to interoperate, rather than having to replace these systems with a common system.[74]

Three types of challenges can be distinguished with federated identity management. First, there are technological and procedural challenges, such as implementing the needed technology, establishing the appropriate processes and procedures; ensuring the interoperability of identity assertion communications between identity providers and relying parties, and ensuring security of subject identity information. The second challenge is economic and involves the costs of deployment, coordination and use of identity management systems. Third, there are legal challenges, relating to privacy authentication, liability, performance.[75]

In order to meet these challenges, each of the parties has to be able to rely on the other roles to perform their obligations. If they fail to do so, there may be harm to the other parties. Smedinghoff gives an overview of the responsibilities of each of the roles in the federated identity management system.[76] Each of these should be taken into account in the use of a federated identity management system in the EGDI. The subject (i.e. the person that is signing on) should provide accurate identity information, and prevent any unauthorised use of any token.[77] The identity provider (i.e. the entity providing the credentials and doing the identification) should properly and accurately identify the subjects, and ensure that all identity assertions are accurately based on current valid information that is properly authenticated. It should develop policies, practices and procedures for the identification processes and comply with them, so that the users can rely on them.[78] Next, it should protect the privacy and security of the subjects' personal data in accordance with its policies, practices and procedures and in accordance with applicable law. Finally, the relying party (the provider of the service for which authentication is required to obtain access) should properly authenticate credentials and any identity assertions before relying on them, and limit its reliance on an identity assertion to what is appropriate for the circumstances (e.g., credentials issued with a low assurance level, such as a library card, should not be relied upon in situations requiring a very high assurance level, such as access to a sensitive military facility).[79]

These obligations could be laid down in a contractual arrangement defining the roles, rights and responsibilities. The Liberty Alliance refers to this as a legally binding Circle of Trust. Such a contractual arrangement would determine the relationship between the participants and with the users and provide the participants with a legally enforceable agreement in case problems may arise.[80] The contract should include provisions on, among others, the roles, rights and obligations of the parties, privacy and security standards, the minimum

[74] R. Morgan et al. (2004). "Federated security: the Shibboleth approach". *Educause Quarterly* 4, 12-17 (hereafter [Morgan et al. 2004]).

[75] [Smedinghoff 2009].

[76] [Smedinghoff 2009].

[77] [Smedinghoff 2009].

[78] [Smedinghoff 2009].

[79] [Smedinghoff 2009].

[80] V. Scheckler et al. (s.d.). *Liberty Alliance Contractual Framework Outline for Circles of Trust*, http://www.projectliberty.org/liberty/content/download/2962/19808/file/Liberty%20Legal%20Frameworks.pdf (accessed on 22/05/2013). (hereafter [Scheckler et al.])

service levels, risk allocation, responsibilities and liabilities.[81] Such a contractual arrangement would guarantee that the governance structure of the EGDI is aware of the technical, legal and organisational issues involved in setting up and maintaining federated identity management in the EGDI. An important issue is who will be responsible and bear the consequences of e.g. acting in reliance on a false identity, or to the contrary, mistakenly failing to accept valid credentials.[82] What is the liability of the identity provider for failing to correctly detect misuse? What is the liability of a relying party for relying on a fraudulent assertion?

Several systems are available on the market for federated identity management. One of the systems that can be used, particularly in the context of an infrastructure that will be used for research, is the open-source Shibboleth system. The main benefit of such a system as Shibboleth is that it combines authentication with the protection of personal data, in that it allows the authentication to be done at the home institution and the authorization to be based on attributes.[83]

2.3.6 Personal data protection

As mentioned earlier, the use of an identity management system implies the processing of personal data. When the choice is made to restrict access to particular data sets or services that are part of the EGDI, this entails that information will be collected and processed on the people that are allowed to access these data or services, when they access it, how many times they access it, etc. A second situation where such information will be collected, is when access to data sets or services is made subject to specific licensing conditions or charges, requiring the provider to know who has accessed and used the data or service, which organisation they belong to, and other metrics that may be relevant for the calculation of the charges, such as e.g. how many bytes of data have been downloaded, how many times the data or service has been accessed, etc. In both situations, personal data is collected. An important part of building trust in the EGDI will be the correct processing of these data, in compliance with the rules and principles of personal data protection.

As there is already an extensive body of literature, reports and guidelines dealing with personal data protection, in this report we will only briefly address the main points of attention for the EGDI. This includes the field of application of the data protection rules, the responsibilities of the controller and processor and the security requirements.

2.3.6.1 Legal framework for the protection of personal data

The EGDI governance structure and/or the data and service providers, depending on how the access management and identity management is organised, will have to comply with the legal framework on privacy and data protection.

This legal framework consists of a number of different regulations:

[81] [Scheckler et al.].
[82] [Smedinghoff 2009].
[83] [Morgan et al. 2004].

- Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[84], which acknowledges the right to respect for private and family life;
- Article 7 of the Charter of Fundamental Rights of the European Union[85], which also recognises the right to respect for everyone's private and family life, home and communications;
- Article 8 of the Charter of Fundamental Rights of the European Union[86], which guarantees the right to protection of personal data;
- Directive 95/46/EC 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 (Data Protection Directive)[87]. This directive is currently in revision and will be replaced by a Regulation.[88]
- Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[89] and its amending acts;
- Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC[90]
- National legislation transposing the directives listed above.

The most important set of rules that need to be taken into account are the provisions from the Data Protection Directive and its national transposition laws. While the main principles that need to be complied with are provided in the directive, the national transposing legislations may have their own definitions and specific rules that need to be taken into account.

[84] Council of Europe (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*, http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (accessed on 22/05/2013).

[85] European Parliament, Council and European Commission (2010). Charter of Fundamental Rights of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF (accessed on 23/05/2013).

[86] European Parliament, Council and European Commission (2010). Charter of Fundamental Rights of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF (accessed on 23/05/2013).

[87] European Parliament and Council (1995). Directive 95/46/EC 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, *OJ L* 281, 23 November 1995, 31-50.

[88] European Commission (2012). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, COM (2012), 11 final.

[89] European Parliament and Council (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), *OJ L* 201, 31 July 2002, 37-47.

[90] European Parliament and Council (2006). Directive of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ L* 105, 13 April 2006, 54-63.

Therefore, it is important that the organisations within the EGDI that are responsible for the processing of personal data first examine which national legislation is applicable. In what follows, we will only discuss the European-wide rules as they are set out in the directive, because it is not possible to examine all national legislations that may be applicable for all the data controllers in the EGDI.

The Data Protection Directive is currently under revision and will be replaced by a Regulation, which will be directly applicable and will not have to be transposed into national legislation, in this way avoiding differences among the national texts. The Regulation is still under discussion, so in the future roll-out of the EGDI, its development will have to be followed up.

2.3.6.2 Definitions: the 'processing' of 'personal data'

The Data Protection Directive is applicable to the "processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system".[91] Two terms that are important in this field of application are 'processing' and 'personal data'.

Personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[92] A person is directly identifiable e.g. by his national identification number or social security number, as such a number is uniquely assigned to one person. Other examples include name, date of birth, address. While the latter are not necessarily unique, they carry a high probability of direct identification.[93] If direct identification is not possible, indirect identification may still take place by combining different elements or deducing different identifiers from other available information. In the EGDI, there may a small opportunity that some large scale geological data may lead to the indirect identification of a data subject. In such cases, these data would have to be treated as personal data. However, while this chance is very slim, the implementation of access control or an identity management system will in most cases involve the processing of personal data, leading to the applicability of data protection principles.

A 'processing' of personal data has to take place. This involves "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".[94] Hence, virtually every act involving personal data is an act of processing. The collection, verification, and authentica-

[91] Art. 3.1 Data Protection Directive.

[92] Art. 2(a) Data Protection Directive.

[93] [Dumortier et al. 2011].

[94] Art. 2(b) Data Protection Directive.

tion of identities, user IDs, passwords and attributes by the EGDI will therefore involve the processing of personal data.

2.3.6.3 Responsible party: the 'controller'

The entity responsible for complying with the rules on data protection is the data controller. It is also the data controller who faces primary liability for any data protection law breaches.[95] A controller is "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".[96] Hence, it is possible that there is more than one controller for the same personal data.

If a controller charges another entity with processing the personal data on its behalf, for example a subcontractor, this entity is known as the data processor. A processor is defined as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".[97]

In such cases, the controller has to choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and ensure compliance with those measures.[98] The contract between the controller and the processor has to be in writing for evidence purposes, and it has to include the obligation for the processor to act only on the controller's instructions and to comply with equivalent safety obligations as those imposed on the controller.[99]

In the EGDI, it will be important to determine which of the actors will act as controller(s) or processor(s). The controller determines the means and purposes of the processing, while the processor executes on behalf of the controller. In principle, the controller is the entity that is responsible for complying with the rules of the Data Protection Directive. However, the contract with the processor may also contain legally binding obligations for the latter. In addition, in some Member States there may be additional liabilities imposed on the processors.[100] It is not always easy to determine which party is the controller and which party is a processor. Therefore, it is important that the specific tasks and responsibilities of each partner are laid down in detail.

2.3.6.4 Applicable national provisions

As the Data Protection Directive does not apply directly, but had to be transposed into national legislation, it has to be checked which national data protection provisions will apply to

[95] W. Kuan Hon et al. (2011). "Who is responsible for personal data in cloud computing? – The cloud of unknowing part 2", *International Data Privacy Law* 2(1), 1-18, http://idpl.oxfordjournals.org/content/2/1/3.full (accessed on 22/05/2013). (hereafter [Kuan Hon et al. 2011])

[96] Art. 2(d) Data Protection Directive.

[97] Art. 2(e) Data Protection Directive.

[98] Art. 17.2. Data Protection Directive.

[99] Cf. infra.

[100] [Kuan Hon et al. 2011].

the processing of the personal data in the EGDI. According to Article 4 of the Data Protection Directive, the provisions of a Member State apply when:

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.

Hence, what is relevant is the place of establishment of the controller. The Data Protection Directive and its national provisions will then apply if the controller is established in the EU and if the controller is not established in the EU but uses equipment located in the EU for processing of personal data (e.g., data centres for storage and remote processing of personal data situated on the territory of a Member State, computers, terminals, servers), unless such equipment is used only for purposes of transit through the territory of the EU.[101]

In the EGDI, the controller will most likely be established in one of the countries of the EU. Then, the national law of this country will apply. If the governance structure of the EGDI would involve entities outside of the EU, it is advisable that the controller always remains an entity established in the EU, and that the personal data are not transferred outside the EU, in order to ensure the compliance with the data protection principles.

2.3.6.5 Principles of data processing

The controller has to comply with a number of main principles for data processing. First, the processing of personal data has to be performed on the basis of a 'legitimate' ground. A closed list of such limited grounds is provided in the Data Protection Directive.[102] Data can only be processed 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

[101] ENISA (2009). Cloud computing. Benefits, risks and recommendations for information security, http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment (accessed on 22/05/2013). (hereafter [ENISA 2009])

[102] Art. 7 Data Protection Directive.

(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) of the Directive.

In the EGDI, there may be a number of grounds applicable, depending on the type of service for which personal data is collected, including consent, the performance of a contract, or compliance with a legal obligation. However, it is recommended that the controller always obtains the consent of the data subjects on which data is collected in the identity management system. The controller has to make sure that the data subject is sufficiently informed about the purpose of the processing for which he or she is giving consent. This consent does not need to be in writing, but for evidence purposes it is to be recommended. The controller in the EGDI should develop a clear consent form and make sure that the data subject has the opportunity to read the information that is given. In an online environment, ideally the data subject can only click an accept or ‘consent’ button after going through the information.

Any collection of personal data has to be performed for clearly specified, explicit and legitimate purposes, and any further processing has to be compatible with these purposes. These purposes and the means of processing have to be determined before the processing starts.

The data need to be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. For example, if in a federated identity management system, if it is sufficient for the service provider to know to which organisation a particular person belongs (e.g. because any employee of that organisation can access them), it does not need to know or collect that person’s name. This principle is often referred to as data minimisation. This also includes that data should be kept in a form which allows identification for no longer than is necessary for the purpose for which they are collected or processed.

The personal data also need to be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

2.3.6.6 Information to the data subject

The controller needs to provide information to the data subject on the processing of his or her personal data. This information includes:

a) the identity of the controller and of his representative, if any;

b) the purposes of the processing for which the data are intended;

c) any further information such as the recipients or categories of recipients of the data; and the existence of the right of access to and the right to rectify the data concerning him or her.[103]

If the information has not been obtained from the data subject itself, but from another entity, the controller still needs to contact the data subject. In such cases the controller has to provide information on

a) the identity of the controller and of his representative, if any;
b) the purposes of the processing
c) any further information such as the categories of data concerned; the recipients or categories of recipients; the existence of the right of access to and the right to rectify the data concerning him or her.[104]

The data subject has a right of access to the data that have been collected about him or her. He or she can ask information about which data have been collected, for what purposes they are processed, and to which recipients they have been transferred. He or she can also ask the communication to him in an intelligible form of the actual data undergoing processing and of any available information as to their source.[105] He or she also has a right to correction and a right to object on compelling legal grounds.[106]

2.3.6.7 Security obligations

Article 17 of the Data Protection Directive requires the data 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."

For the implementation of measures to ensure an appropriate level of security in relation to the risks to the personal data, the state of the art and the cost of the implementation of the measures are taken into account.

In addition, under Article 16, the Data Protection Directive makes clear that only authorised persons should be granted access to personal data stored for processing. In addition, for these persons it should be decided what level of processing they are allowed to do with the data they have access to. This is based on the general proportionality principle of data protection.[107]

2.3.6.8 Notification to the Data Protection Authority

Before carrying out a personal data processing operation, the controller has to notify the Data Protection Authority of his Member State that this processing is taking place and he

[103] Art. 10 Data Protection Directive.
[104] Art. 11 Data Protection Directive.
[105] Art. 12 Data Protection Directive.
[106] Art. 14 Data Protection Directive.
[107] [Dumortier et al. 2011].

has to provide information to the Data Protection Authority on the identity of the controller, the purpose of the processing, which data subjects and which personal data will be involved, the recipients of the data, the proposed transfers to third countries, and a general description of the technical and organisational measures that will be taken to protect the security and confidentiality of the personal data.

2.3.7 Impact on the EGDI

In setting up the EGDI, the data and service providers and/or the EGDI governance structure that will be developed, have to assess for which data and services they want to introduce an identity and access management system, and which level of assurance this identity management system must give. On the basis of this assessment, there will be a number of points of attention:

- Identity management system: an appropriate identity management system needs to be set up, that allows for cross-border transactions, and that does not impose too heavy a burden on the users of the system (e.g. often qualified electronic signatures are too 'heavy'). A federated identity management should be considered, and the appropriate software, policies and security for this should be agreed upon. It should be considered whether a third party will be the identity provider, or whether one of the entities in the EGDI will function as the identity provider. Tasks and responsibilities for managing this federated identity management should be allocated in an agreement between all parties in the EGDI that will use the system.
- Personal data protection: for the processing of personal data from the identity management system, the tasks and responsibilities should be clearly set out and a controller should be assigned. This controller should make sure that
    - It is clearly established which national data protection legislation is applicable;
    - A privacy policy is drafted for the EGDI that includes a division of tasks and responsibilities, and organizational and technical measures for the treatment, confidentiality, and security of the personal data. This privacy policy should be disseminated to all partners in the EGDI;
    - Consent is obtained in writing from the data subject by using an appropriate standard form for consent;
    - The purpose of the processing is legitimate and clearly delineated before the collection of the personal data starts, and the data are not used for any other purpose than the purpose that is communicated to the data subjects. This purpose will be the provision of the data and services, and making sure that only authorised persons get access to these data and services.
    - Only the data that are strictly necessary for the purpose can be collected and processed. They have to be destroyed as soon as they are no longer necessary for the purpose.
    - The data subjects are appropriately informed about the data processing and about their rights to access, correction and objection.
    - The personal data are processed on the territory of a European Member State and not transferred to a country that does not have an adequate level of data protection;

- The competent national Data Protection Authority is notified about the data processing operations.

3 Moving the EGDI to the cloud

Many public sector organisations have decide to use cloud services for their activities or are contemplating this move. This could also be a possibility for the EGDI. To a certain extent, the EGDI can already be considered a form of cloud in itself, but it can also consider involving cloud services from private sector vendors. This may have considerable benefits relating to scalability and efficiency. However, there are a number of risks and possible disadvantages that need to be taken into account. This section will address some of the potential risks of moving the EGDI to the cloud, and examine a concrete example, i.e. moving the data held in the EGDI to Google. First, we will give a short overview of the main characteristics of the cloud.

3.1 The cloud

There are many definitions of the cloud, but one that is generally adopted is the definition from the United States National Institute of Standards and Technology: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[108]

Generally, a distinction is made between three service models.

- Software as a service (SaaS): software or applications offered by a third party provider, available on demand.[109] This is the most commonly known form of cloud services, including examples such as Google Docs, Salesforce, Hotmail, or Facebook. The consumer does not have any control over the underlying cloud infrastructure including network servers, operating systems, storage or application capabilities.[110]
- Platform as a service (PaaS): the cloud user can deploy onto the cloud infrastructure its own created or acquired applications, using programming tools supported by the provider. An example is Google Apps. Again, the consumer does not have any control over the underlying infrastructure including the network, the servers, operating systems or storage, but it does have control over the applications.[111]
- Infrastructure as a service (IaaS): the cloud user is provided with processing, storage, network and other fundamental computing resources on which it can deploy and run software, including operating systems and applications. Hence, the user has more control over operating systems, applications and storage, but does not control the underlying infrastructure.[112]

A second distinction is made between three types of clouds:

[108] P. Mell and T. Grance (2011), *The NIST definition of cloud computing,* *http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf* (accessed on 22/05/2013).

[109] [ENISA 2009]; C. May (2013). "Seeing into the Cloud: How to Mitigate Potential Ethical and Security Issues, *Federal Lawyer* 60, 69-76. (hereafter [May 2013]).

[110] [Soma et al. 2011].

[111] [Soma et al. 2011].

[112] [Soma et al. 2011].

- Private cloud: the cloud infrastructure is set up for and used by one single organisation.[113] It can be managed by the organisation itself or by a third party, and it can be set up either at the premises of the organisation or remotely.
- Community cloud: the infrastructure is shared by a number of organisations that share particular concerns e.g. relating to security requirements,[114] or compliance with specific legislation, e.g. in the health-care sector or financial sector.
- Public cloud: the infrastructure is available to anyone wishing to enter into a contract with the cloud provider.

In some cases, two or more of these models may be combined into a hybrid cloud, in which the models are bound together by standardized or proprietary technology that enables data and application portability.[115]

Depending on the models, the benefits and risks, but also the division of responsibilities and liability between the cloud user and cloud provider will be different. In the framework of the EGDI, the EGDI governance structure will have to decide whether to 'put its data in the cloud' and which type of cloud it will use. For instance, in an IaaS model, the cloud provider will typically only be responsible for the physical security of the environment and the availability of the infrastructure, such as network connectivity, or server availability. The security of the applications and databases is the responsibility of the cloud user.[116] In the case of PaaS, the user will be responsible for the applications, but not for the software tools provided to build these applications, while in SaaS models, the provider will be responsible for security and the proper working of the applications.[117] Next, the advantage of a private cloud will be the smaller risk for security breaches or data loss, and no need for sharing processing resources with other "tenants" of the cloud. However, using a public cloud may incur lower costs and larger flexibility. On the other hand, the public cloud may allow less room for negotiating the Service Level Agreement and other terms and conditions between the user and the provider. A balance needs to be sought between the benefits of the envisaged cloud services and their risks. These benefits and risks will be discussed in the next sections.

3.2 Benefits of the cloud

Benefits of the cloud are manifold, including reduced cost, pricing flexibility, agility, and risk-reduction.[118]

The cloud user can significantly reduce its investment in IT infrastructure and equipment, and move to a pay-for-use model rather than a fixed-cost structure.[119] This is also true for

[113] [May 2013].

[114] [Soma et al. 2011].

[115] [Soma et al. 2011].

[116] [Soma et al. 2011].

[117] [Soma et al. 2011].

[118] [Soma et al. 2011].

[119] [Soma et al. 2011]; T. Martin (2010). "Hey! You ! Get off my cloud: defining and protecting the metes and bounds of privacy, security, and property in cloud computing", *Journal of the Patent and Trademark Office Society* 92, 283-314. (hereafter [Martin 2010])

governments: the cost of government ICT can be reduced, leaving more resources for fulfilling the core missions of government agencies.[120] Cloud services can also provide more cost-effective storage for logs, allowing more comprehensive logging without compromising performance.[121] In addition, the user does not need to acquire the specific IT-skills required for maintaining the infrastructure, but can rely on the specialist knowledge available at the cloud provider.

Cloud computing also has practical and technical advantages: possible peaks in processing loads and under-utilization of processing power in off-peak moments can be handled and diverted by the cloud provider. The users can get to their data from anywhere with an internet connection.[122] The decentralisation of data by cloud providers leads to greater redundancy, benefits of scale for security measures (e.g. through content replication, federated identity management, or efficient role-based access control)[123] and less vulnerability to external events such as natural disasters.[124]

3.3 Risks of the cloud

A considerable body of research has developed with regard to the possible risks related to the use and provision of cloud services. This report will not repeat all the risks that were identified, but rather refer to the extensive analysis done by ENISA in its 2009 report “Cloud computing. Benefits, risks and recommendations for information security”.[125] In this section, we will only give a general overview of the risks that may be of importance for the EGDI.

These risks may even be intensified if the EGDI uses multiple cloud service providers, e.g. because of procurement rules. In such cases, the EGDI will end up with a heterogeneous environment of different types of cloud services from multiple cloud service providers.[126]

3.3.1 Security and continuity

Using cloud services raises concerns for security and continuity, because the user will depend on the cloud service provider’s security measures, and in most cases will not be able to impose any security requirements. Inadequate security may lead to loss of data, corruption of data, problems in extracting the data from the cloud service, unintended exposure of

[120] S. Ahmed (2010). “Data portability: key to cloud portability”, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1712565 (accessed on 22/05/2013) (hereafter [Ahmed 2010]); RAND (2010). *The Cloud: Understanding the Security, Privacy and Trust Challenges*, http://www.rand.org/pubs/technical_reports/TR933.html (accessed on 22/05/2013). (hereafter [RAND 2010])

[121] [ENISA 2009].

[122] European Commission (2012). Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the potential of cloud computing in Europe, COM(2012) 529 final (hereafter [European Commission 2012a]; [Martin 2010].

[123] [ENISA 2009].

[124] [Martin 2010].

[125] [ENISA 2009].

[126] [Ahmed 2010].

data, or continuity problems.[127] This may cause reputation damage, or contractual liability of the cloud user towards its end-users.[128]

An important element in the security policy is the need for secure authentication measures. As was mentioned earlier, authentication and authorisation processes are important to make sure that the data and services in the EGDI are used only by the persons who are authorised to do so. This becomes even more important in the cloud. As the European Commission stated in its Communication on Cloud Computing: "The more complex value chains and the nested nature of many services in cloud computing makes reliable authentication necessary both to secure trust and to streamline the use of the services. For example single sign-on procedures make the use of a set of services much smoother but require more sophisticated and reliable authentication methods than simple self-created passwords to enhance trust in the set of providers concerned. The adoption of common standards that permit safe but seamless use of services requiring reliable authentication and authorisation would be a major boon to cloud adoption".[129]

The cloud user has to take a proactive approach in assessing the appropriateness of the cloud provider's security measures in relation to the sensitivity of the data involved, and of course take its own security measures where possible.[130] The EGDI should clearly define its security requirements and select a cloud service provider that can meet these requirements.[131] In this selection, financial interests have to be weighed against the need for security guarantees, the need for uninterrupted services and business continuity. ENISA has developed a checklist of questions that can be used by cloud users to select the cloud service provider that could best meet their needs. This checklist can be a valuable guideline in the EGDI's selection process.[132]

In selecting the cloud services provider, the service level agreement will play an important role: what kind of guarantees is the cloud service provider giving for the data and services to be at the disposal of the cloud user and its end users at any moment they require? However, few cloud service providers are willing to guarantee the availability of service levels taking responsibility for internet performance, for instance in the case of denial of service attacks.[133] Moreover, many cloud service providers limit or exclude their liability or any problems that may occur.

While in many cases, the cloud user may not be able to negotiate its contract with the cloud provider and will have to agree to the standard terms and conditions imposed by the cloud provider, large users may have the possibility to negotiate different terms. Considering the amount of data and services that will be part of the EGDI, it is suggested that any bargaining power is used to ensure the continuity of the service of the cloud provider. This may be

[127] [Ahmed 2010].

[128] A. Joint and E. Baker (2011). "Knowing the past to understand the present - issues in the contracting for cloud based services", *Computer Law and Security Review* 27(4), 407-415. (hereafter [Joint and Baker 2011])

[129] [European Commission 2012a].

[130] [Soma et al. 2011].

[131] [Ahmed 2010].

[132] [ENISA 2009].

[133] [Joint and Baker 2011].

required to guarantee the service levels demanded by the INSPIRE requirements or under the EGDI's own service level agreements or terms of service. Other elements that may be important to negotiate are the right to be notified of security incidents and the timeframe of notification[134]; prior notification of maintenance downtime, changes to the service, etc.[135]

3.3.2 Personal data protection

A particular concern regarding security relates to the protection of personal data, as the processing of such data has to comply with specific requirements under the Data Protection Directive.[136] While the data included in the EGDI will in most cases not contain personal data, as discussed above the possible use of identity management processes for managing access to confidential or restricted datasets will most likely imply that personal data will be collected from the users accessing the geological data or services. If these data are stored in the cloud, the EGDI will have to make sure that the applicable legislation on privacy and data protection is complied with.

One of the main questions in the context of cloud computing involves the division of responsibilities and liability between the different actors in the cloud computing value chain, and the determining of the processors and controllers of the data processing operations and their obligations.[137] Cloud computing is blurring the distinction between both actors.[138] According to the Article 29 Working Party's Opinion 169, what matters most in determining who the controller is, is factual control, and not contractual provisions or labels, although the contract terms still may be important.[139] The entity that determines either the purposes of processing or the 'effective means' of processing is a controller. These 'effective means' are considered by the Working Party as the substantial questions that are essential to the core of the processing: which data to process, for how long, which third parties will have access to the data, when will the data be deleted, etc. The technical and organisational questions can be delegated to the processor, without turning him into a controller. For the technical and organisational measures for security, it is still under discussion whether a decision on this makes an entity a controller or not, because even though it is a technical measure, security has become essential.[140]

Are cloud providers processors on behalf of the cloud user-controller? Some argue that storing data as a host without knowing that it contains personal data should not be considered processing.[141] However, data replication for business continuity purposes, splitting

[134] W. Kuan Hon et al. (2012). "Negotiating cloud contracts: looking at clouds from both sides now", *Stanford Technology Law Review* 16, 79-128. (hereafter [Kuan Hon et al. 2012]).

[135] [Kuan Hon et al. 2012].

[136] Cf. supra.

[137] [European Commission 2012a].

[138] [Kuan Hon et al. 2011]; P. Balboni (2010). "Data protection and data security issues related to cloud computing in the EU", *Tilburg University Legal Studies Working Paper Series*, http://ssrn.com/abstract=1661437 (accessed on 22/05/2013).

[139] Article 29 Working Party (2010). *Opinion 1/2010 on the concepts of "controller" and "processor". Opinion 169*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (accessed on 22/05/2013).

[140] [Kuan Hon et al. 2011].

[141] [Kuan Hon et al. 2011].

personal data into fragments may be considered processing operations which qualify the cloud service provider as a processor.[142] At the moment, the full extent of the cloud service provider's obligations relating to personal data is still unclear.

Putting personal data in the cloud entails a transfer of personal data to third parties under the Data Protection Directive, possibly to countries outside of the European Union. This implies not only that the data subject has to be informed about this by the cloud user, but also that the provisions of the directive will apply for transfer of data. In the cases where the data is transferred to a country outside of the European Union, Article 26 of the Data protection Directive will have to be taken into account, requiring particular safeguards for the protection of the personal data.

The EGDI governance structure will have to evaluate in how far the cloud service provider can guarantee the compliance with the EU data protection rules. Some cloud service provider allow the users to choose where their data are stored, enabling the data to remain in the European Union.[143] As some data providers in the EGDI may also be confronted with other requirements for government-held data to stay within the EU or their own country, if possible the EGDI governance structure should make sure that it can choose the storage location.

3.3.3 Control and ownership

The EGDI governance structure and the data providers must carefully consider the provisions in the contractual agreements with the cloud service provider relating to ownership and use of the data they decide to store in the cloud. First, it should be checked what kind of rights the cloud service provider will claim during the course of the contract. Some cloud service providers reserve the right to use the cloud user's data for their own business purposes to different extents depending on the wording of their terms of use. This may be a problem in the case of confidential data or data to which access is restricted, e.g. for national security reasons. Linked to this, it also has to be checked to what extent the cloud service provider has access to the data for monitoring or maintenance purposes and for which purposes it can use any resulting information.[144]

Sometimes, the cloud service provider also wants to retain the right to use data from the cloud user even after the contract has terminated. If possible, it should be made sure that the data is properly deleted after the end of the contract, after an appropriate transition period. However, this may be difficult, for example when full deletion is only possible by destroying a disk which also stores data from other cloud users, or there is no true data wiping.[145]

3.3.4 Interoperability and portability

As cloud services are not fully developed yet, there may still be a lack of interoperability between the services offered by the various cloud providers. If the cloud service does not

[142] [Kuan Hon et al. 2011].

[143] [Kuan Hon et al. 2012].

[144] [Kuan Hon et al. 2012].

[145] [ENISA 2009].

allow for the efficient migration of the data, whether for technical or policy reasons[146], this may cause problems for the cloud user to move to another cloud provider or to integrate data or services. With regard to moving the data, this issue is often referred to as data portability.[147]

If the EGDI intends to use cloud services, it has to be ensured that appropriate ‘exit arrangements’ are made for the transition to another cloud service provider, to avoid ‘vendor lock-in’.[148] These arrangements need to include details of the file formats the data will be returned in; the grant of any licences needed to access that data; details on how the data will be made available; and a timeline for the transition. It should be the aim to ensure that the provider complies with commonly agreed upon standards and formats, allowing the EGDI data providers to transfer their data and services to another provider if they wish to do so later on. In this way, unreasonable dependence on a cloud service provider can be avoided.[149]

3.3.5 Audits

In some cases, an EGDI entity may be required to perform an audit in order to prove its compliance with particular standards or national regulation. Such audits may become more difficult when the data, services or processes that need to be audited are controlled by the cloud provider. Research shows that cloud providers are not inclined to allow such audits, for reasons of security and costs.[150]

In case such audits are possible, there may still be challenges. With regard to the integrity of the data, it may also be difficult to ensure audit trails showing that modifications to the data took place at a particular time or on a particular device within the cloud.[151]

3.3.6 Jurisdiction and applicable law

All the risks mentioned above have to be seen against the background of the more horizontal risk that threatens all the legal requirements and compliance questions: jurisdiction.[152] If data and services are put in the cloud, it is very difficult to find out which law is applicable and which court will be competent to handle any disputes. Where are the servers located storing the data? Is all the data kept in one place or is it transferred, based on performance efficiency? It may be difficult to determine the place of establishment of the cloud service provider.[153] Moreover, to what extent does compliance with the applicable law in the place

[146] [Ahmed 2010].
[147] [Ahmed 2010].
[148] [Joint and Baker 2011].
[149] [Ahmed 2010]. For a detailed overview of the consequences of vendor-lock per type of cloud service (SaaS, PaaS, IaaS), see [ENISA 2009].
[150] [Kuan Hon et al. 2012].
[151] M Taylor and M. Matteucci (2010). “Cloud computing”, *Computer and Telecommunications Law Review*, 57-59.
[152] [RAND 2010].
[153] [European Commission 2012a].

where the cloud service is offered suffice for the cloud user to meet its requirements of compliance with the applicable law where the end user accesses the data and services?[154]

Applicable law and jurisdiction are often laid down in the standard terms of the cloud service provider, without room for negotiation. If there is no provision on applicable law in the agreement, the Rome I Regulation will apply, entailing that the law of the country with which the contract is most closely connected will be applicable. Jurisdiction will be settled by the Brussels I Regulation. However, determining this may be complicated by the fact that the cloud service provider will himself not always be able to identify the exact location of an individual data set or the assets of an individual customer. In addition, finding this out or allowing the customer to access this location or to perform its own audits, may breach the confidentiality and security requirements of other users.[155]

If possible, the EGDI governance structure should try to negotiate the applicable law and jurisdiction, to at least a country within the European Union.

3.4 Impact on the EGDI

In making its decision on "moving to the cloud", the EGDI governance structure should make a thorough assessment of the advantages and the risks involved, in cooperation with the data and service providers involved in the EGDI. It should compare the services available on the market, and assess in how far they comply with the EGDI's requirements from a technical, organisational and legal perspective. ENISA has designed a set of assurance criteria designed to:

1. Assess the risk of adopting cloud services (comparing the risks in maintaining a 'classical' organisation and architecture with the risks of migrating to a cloud computing environment);
2. To compare different cloud provider offers;
3. To obtain assurance from the selected cloud providers;
4. To reduce the assurance burden on cloud providers, who would now not have to deal with individual requests for audits of their infrastructures and policies.[156]

These criteria would be useful for the EGDI to use as guidelines for their evaluation of potential cloud service providers. The questions developed by ENISA look at issues such as personnel security; supply-chain management, operational security; authorization and authentication; asset management; continuity management; physical security; and legal requirements.[157]

In as far as possible, the EGDI governance structure should negotiate with the cloud service providers so that the requirements of the infrastructure, the data and service providers, and the end users can be met. Points of negotiation could include, among others, exclusion

[154] [Joint and Baker 2011].

[155] [Joint and Baker 2011].

[156][ENISA 2009].

[157] [ENISA 2009]; J. Garon (2011). "Navigating through the Cloud – Legal and Regulatory Management for Software as a Service", *NKU Chase Law & Informatics Institute Working Papers Series*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2025246 (accessed on 22/05/2013).

or limitation of liabilities and remedies; service levels, including availability; security and privacy, particularly relating to the Data Protection Directive; lock-in and exit arrangements; providers' ability to change service features unilaterally; intellectual property rights; applicable law and jurisdiction.[158]

3.5 Case study: Google

One possibility for the EGDI to use the cloud for providing data and services to professional users and end users would be to 'put the data in Google'. For instance, a number of transport authorities have provided their routes to Google to be included in Google Maps and almost 40 years of satellite imagery data from Landsat is available on Google Earth Engine.[159] Concluding an agreement with Google would be beneficial for EGDI in that it would make available Google's large storage capacity and processing power, and allow the EGDI to offer very powerful and fast services to its users. However, there might also be drawbacks, in the form of use conditions that have to be agreed with. These use conditions may have comparable risks to those that were described in the previous chapter on cloud services. It will be up to the decision-making entities within the EGDI to assess the possible consequences of entering into an agreement with Google, to try to negotiate on these conditions, or to decide whether or not to accept the conditions that are non-negotiable.

Google has developed a number of enterprise mapping products that could be used by the EGDI to make its data and services available. In essence, there are two ways of partnering with Google. First, an organisation can submit content to Google, so that it can be viewed by the public, e.g. on Google Maps. Second, an organisation can use the enterprise products for e.g. planning and analysis, emergency management or offering services to end-users.

In the following sections, we give an overview of the possible conditions that may apply to using Google as a cloud service provider. The description below is based on information that could be found on Google's web pages. However, in many cases the information needed to get a full picture of the contractual rights and obligations can only be obtained by contacting Google's sales department. It is recommended that for any specific information, the EGDI entities contact a Google representative.

3.5.1 Submitting content to Google

Google has made it possible for public bodies to submit their content to Google to be displayed in Google Maps, Google Earth, etc.[160] Via the Map Content Partners programme, organisations with authoritative data can make their data available to the worldwide public. Data that can be provided include base map (vector) data; cities in 3D; imagery; and transit information.[161] Specifically, the following types of data are accepted by Google:

- 3D building models

[158] [Kuan Hon et al. 2012].

[159] See http://earthengine.google.org/#intro.

[160] See http://www.google.com/submityourcontent/public-agency/.

[161] See http://www.google.com/help/maps/mapcontent/.

- Aerial imagery (current and historical)
- Digital terrain models
- Public transit system routes and schedules
- Parks and protected areas
- Places of interest (hospitals, tourist attractions, government buildings)
- New developments/construction (residential neighborhoods, shopping centers)
    - Road networks
    - Geocoded addresses
    - Parcel data
- Building footprints
- Bike paths[162].

The specifications for each of the content types are set out in detail on the programme's website.[163] In order to upload the data, the organisation needs to contact Google via filling out a web form.[164]

In order to add the organisation's content to Google, a content licence agreement needs to be entered into, affirming that the organisation has the necessary rights to grant a licence to the content and determining what Google will and won't do with the content.[165] In case the content is in the public domain, no licence agreement is necessary.

The licence agreement itself is not available publicly and is only provided to organisations that have contacted Google for uploading their data. Therefore, it is impossible to assess all conditions of the agreement. In fact, Google asks its partners not to disclose the terms of the agreement.[166]

However, some things are already clarified in the information on the Map Content Partners Programme's website. For instance, the licence agreement is not an exclusive agreement, and the content provider can still disseminate its information via other channels.[167] However, Google does get a perpetual and irrevocable right to maintain the content in its services, entailing that the provider cannot ask to remove its data later on. Google does not resell or redistribute the content, but it is viewable in free consumer services such as Google Maps, which incorporates advertising, and Google Earth Enterprise, which is licensed to organisations at a charge. Some map content will also be made viewable on third party websites through the Google Maps API, but it remains hosted on Google servers and is not redistributed. The raw data is not provided to third parties.

Partners are neither charged nor paid for providing the data. Attribution for the content viewed on Google Earth is done at the base of the user interface, while for Google Maps the attribution is generally put on the legal notices page.[168] In case of public security or

[162]See https://support.google.com/mapcontentpartners/answer/142890?hl=en&ref_topic=21600.
[163] See https://support.google.com/mapcontentpartners/answer/144284.
[164] See https://support.google.com/mapcontentpartners/contact/mapcontent.
[165]See https://support.google.com/mapcontentpartners/answer/144393?hl=en&ref_topic=21599.
[166] See https://support.google.com/mapcontentpartners/answer/146442?hl=en&ref_topic=21682
[167] See https://support.google.com/mapcontentpartners/answer/143976?hl=en&ref_topic=21599.
[168] See https://support.google.com/mapcontentpartners/answer/143993?hl=en&ref_topic=21609.

national safety concerns, Google is willing to discuss possible blurring measures or other security measures.[169]

In principle, the terms of the content licence agreement are non-negotiable. Google offers a version of the licence agreement that is tailored to address common legal concerns of public sector entities that, depending on the country, may have the form of a click-to-accept licence, or be a conventional paper agreement.[170]

3.5.2 Using Google services

In the second situation, the EGDI would not be submitting its content to Google to show it in Google's mapping products to the Google users, but would rather use Google products to develop its own products and services towards its users. Products that may be used include the enterprise versions of Google Maps and Google Earth, and the Google Cloud Platform. In this section, we look at the use conditions for these services.

3.5.2.1 Google Cloud Platform

The Google Cloud Platform includes a number of services:

- Google App Engine: a platform as a service to build and host applications on the same infrastructure used at Google.[171]
- Google Compute Engine: an infrastructure as a service that lets users run their large-scale computing workloads on Linux virtual machines hosted on Google's infrastructure.[172]
- Google Cloud Storage: allows storage and access management for users' data, e.g. for archive purposes, for sharing data, for storing application data, for serving static data for websites.[173]
- Big query: a data analysis service for analysing big data in the cloud using SQL, enabling 'real-time business insights in seconds".[174]
- Cloud SQL: allows maintaining and administering MySQL databases in Google's cloud.[175]
- Google Prediction API: allows using Google's machine learning algorithms to analyse data and predict future outcomes.[176]
- Google Translate API: can be used to build multilingual apps and programmatically translate text in webpages or applications.[177]

Separate terms of service are applied for the Google Apps Engine and the Google Translate API. For Google Cloud Storage, Google Prediction API, Google BigQuery Service,

[169] See https://support.google.com/mapcontentpartners/answer/143998?hl=en&ref_topic=21609.
[170] See https://support.google.com/mapcontentpartners/answer/143977?hl=en&ref_topic=21599.
[171] See https://cloud.google.com/products/.
[172] See https://cloud.google.com/products/compute-engine.
[173] See https://cloud.google.com/products/cloud-storage.
[174] See https://cloud.google.com/products/big-query.
[175]See https://cloud.google.com/products/cloud-sql.
[176] See https://cloud.google.com/products/more-products.
[177] See https://cloud.google.com/products/more-products

Google Cloud SQL, Google Compute Engine, and Google Cloud Datastore, the terms of service are the same.[178] However, the content of the terms of service is largely similar, so they will be discussed together. In order to find the terms of service, a user has to sign in to get started.

The terms of service for Google App Engine are agreed upon by the Customer by ticking the box that he or she has accepted them. The licence works in two directions. On the one hand, the customer obtains a licence to use the service and to integrate the service into any application and provide the integrated product to users. On the other hand, by submitting, posting, generating or displaying and application and/or customer data on or through the service, the customer gives Google the right to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any application and/or including customer data for the sole purpose of enabling Google to provide the customer with the service in accordance with the Agreement. This entails that Google can do whatever is needed with the customer data and the application to make sure its service works. Other than this, Google obtains no rights to the customer's content or any intellectual property.

With regard to security, Google commits to ensuring that all facilities used to store and process applications and customer data will adhere to reasonable security standards no less protective than the security standards at facilities where Google processes and stores its own information of a similar type. As a practical matter, this creates a strong incentive for Google to be constantly improving the data security for its customers because it has strong business incentives to protect its own data. For instance, Google Cloud storage supports OAuth 2.0 authentication, developed by the Internet Engineering Task Force.

The terms of service of the Google App Engine state that Google may process and store applications and customer data in the United States or any other country in which Google or its agents maintain facilities. This may be problematic for public authorities who are required to store their data in their own country. However, with regard to the end user data, Google allows the customer to select the location of storage, either in the United States or the European Union. This enables the customer to comply with its obligations regarding the protection of personal data. In addition, Google is enrolled in the U.S. Safe Harbor programme, so it complies with article 25 of the Data Protection Directive. For the other services, including storage, the customer can choose the storage location for all data.

The terms of service can be altered by Google, and material changes will become effective 90 days after they are posted except if the changes apply to new functionality in which case they will be effective immediately. The customer can only show his disagreement with the changes by stopping to use the service. Modifications will be posted on the website of the Terms of Service, so it is the customer's responsibility to check regularly whether Google had made changes to the agreement.

Material changes to the service itself will be notified by Google, but only if the customer has subscribed with Google to be informed about the change. If Google intends to discontinue the service or make backwards incompatible changes, Google will announce this and use commercially reasonable efforts to continue to operate the service without the changes until

[178] See https://developers.google.com/cloud/terms.

one year after the announcement or April 20, 2015. Exceptions to this are the situation where the discontinuation or change is required by law or a third party relationship, or where waiting this long would create a security risk or substantial economic or material technical burden.

Finally, Google makes no warranties about the service except what is expressly stated and limits its liability for any damages or losses to the maximum extent allowed under the applicable law. The applicable law is the law of the State of California.

The service level agreements are not included in the terms of service, but are provided on a separate webpage.[179] For the Google Apps Engine, Google guarantees an uptime of 99.95% in any calendar month. If it does not reach this limit, customers can claim back a percentage of their bill, based on the downtime percentage. For the standard storage class of Google Cloud Storage, an uptime of 99.9% is guaranteed, and for the Durable Reduced Availability Storage class, the lower limit is 99%.[180]

3.5.2.2 Google Earth and Maps Enterprise

Google Earth and Maps Enterprise includes a number of products:

- Google Maps API for business: this is a collection of APIs that enable the user to overlay his own data on a customised Google Map. Contrary to the free Google Maps API, the API for business includes a service level agreement. In addition, it contains a number of extra features.[181]
- Google Earth Enterprise: this service allows users to store and process terabytes of imagery, terrain and vector data on their own server infrastructure. Users can publish maps securely for their users to view using Google Earth desktop or mobile apps, or through their own application using the Google Maps API.[182]
- Google Maps Engine: this service allows the user to create his own maps and share them with others.[183]
- Google Earth Pro: this is a 3D interactive globe that can be used for data visualisation to aid planning, analysis and decision making.

The terms of service (which were again difficult to find), are discussed below.

Google Maps API for business

Under the agreement, which is entered into by a corresponding Ordering Document, the customer gets a licence to use the Google Maps services to display the maps and track assets in his own implementation and to “access, use, publicly perform and publicly display the Content in the Customer Implementation”.[184]

[179] See https://developers.google.com/appengine/sla; https://developers.google.com/storage/docs/sla; https://developers.google.com/bigquery/sla; https://developers.google.com/compute/docs/sla;

[180] See https://developers.google.com/storage/docs/sla.

[181] See http://www.google.com/enterprise/mapsearth/products/mapsapi.html.

[182] See http://www.google.com/enterprise/mapsearth/products/earthenterprise.html.

[183] See http://www.google.com/enterprise/mapsearth/products/mapsengine.html.

[184] See https://developers.google.com/maps/documentation/business/support#terms_of_use.

If the customer submits his own content to Google through the API services, Google is granted a licence to "reproduce, adapt, modify, translate and distribute this Customer Content". Hence, Google can use the customer's data that are uploaded to be displayed on Google Maps.

Commercially reasonable changes can be made by Google to the service. Material changes will be notified by Google, but only if the customer has subscribed with Google to be informed about the change. The same conditions apply to changes in the terms of service. However, as the customers are paying a fee, Google is slightly more lenient with regard to the possibility of opposing the changes. If the change has a material adverse impact on the customer and he does not agree to the change, he must notify Google within thirty days after receiving notice of these changes. In that case, the customer will remain governed by the terms in effect immediately prior to the change until the end of the license term. Renewal of the licence term would be under the new terms of service.

With regard to deprecation, a comparable policy is in place as for the Google Cloud Platform. Google will announce if it intends to discontinue or make backwards incompatible changes to its APIs or services. Unless a different deprecation period is indicated by Google in writing in the applicable API's or service's agreement or policies, Google will use commercially reasonable efforts to continue to operate the applicable APIs or services without these changes until one year after the product's deprecation announcement. Exceptions to this are the situation where the discontinuation or change is required by law or a third party relationship, or where waiting this long would create a security risk or substantial economic or material technical burden.

The agreement contains detailed provisions on the restrictions of the rights of the user and the payment arrangements. The licence is concluded for a particular term agreed upon by the parties, and is renewed automatically.

A service level agreement, guaranteeing 99.9% uptime for each calendar month, is set out on a separate webpage.[185]

Google Maps Engine API

This API falls under the general terms of service for Google APIs, unless there is a direct licence entered into by the organisation. It is not clear what this direct licence would cover and how it can be obtained. For more information about such licences, Google's sales department needs to be contacted.

For the Google Maps Engine API, the user has to provide the following rights to Google: "By submitting, posting or displaying content to or from the APIs through your API Client, you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute such content. However, Google will only use such content for the purpose of enabling Google to provide the APIs and only in accordance with the applicable Google privacy policies. You agree that this license includes a right for Google to make such content available to other companies, organizations or individuals with whom Google has relation-

[185] See http://www.google.com/enterprise/earthmaps/legal/us/maps_sla.html.

ships for the provision of syndicated services, and to use such content in connection with the provision of those services. Before you submit content to our APIs through your API Client, ensure that you have the necessary rights (including the necessary rights from your end users) to grant us the license".

Google Earth Pro

Google Earth Licences can be bought online.[186] However, the terms of use are not available on this site. They have to be read elsewhere, and it seems that they don't have to be accepted before buying the software.[187] Under the licence, the user obtains the right to use the during the term of the agreement on a single designated computer. Company use is not foreseen.

Google Earth Enterprise

Google Earth Enterprise is specifically designed for customers owning very large quantities of data, such as the EGDI. However, there is no information on the applicable licences available and the sales department has to be contacted for more information.[188]

3.5.3 Impact on the EGDI

If the EGDI governance structure would decide to use Google for the storage of its data or the dissemination of its data and services, it is recommended that they contact a sales representative of Google. The terms of service and licence conditions that can be found on Google's website are not directed at large corporate or government users such as the EGDI, and a separate agreement will have to be made with Google. This may also imply that Google will claim less rights on the data stored on its servers than it does in the case of non-business users of the free services.

In any case, it must be made sure that the EGDI data and service providers can comply with their obligations under European and national law with regard to the storage and dissemination of geological data, that the data are sufficiently secure, and that an appropriate access management control system can be implemented to ensure that possible access restrictions required by national law can be maintained.

[186] See https://earthprostore.appspot.com/check-out.ep.
[187] See http://earth.google.com/intl/en/licensepro.html.
[188] See http://www.google.com/enterprise/mapsearth/products/earthenterprise.html.

4 Conclusion and summary

At the start of setting up the EGDI and during the deployment of the EGDI, the entities involved will have to make a risk assessment, estimating the potential risks to the trust in the EGDI and setting out possible remedies to mitigate these risks.[189] It should also be kept in mind that these risks evolve – for instance, security mechanisms that were state of the art two years ago may be considered easy to breach now. Therefore, an evaluation is necessary every few years.[190]

Many of the topics addressed in this deliverable have an impact on the technical infrastructure of the EGDI. However, as was mentioned a number of times, issues such as security, authentication, data protection or rights management, also have a governance component. The governance model of the EGDI will therefore also play in important role in ensuring trust in the infrastructure and its components, including the different entities involved in the EGDI, their internal organisation and the organisation of their multi- and/or bi-lateral relationships.

In addition, one should not forget the human factors that play a role in trust: systematic attention for the actors in the system or infrastructure from the perspective of their culture and behaviour is just as important as technological security measures or carefully designed trust policies.[191]

In summary, the following points of attention can be given for the inception and implementation of the EGDI.

Trust in the data

1. Metadata: It is recommended that for the non-INSPIRE data sets included in the EGDI, it is examined in how far the metadata requirements of INSPIRE can also be applied. Next, it should be examined in how far the metadata can include information on the fitness for purpose.

2. Quality information: the data providers in the EGDI should consider whether it would be useful and feasible to design a standard method for the description of quality of the geological data included in the EGDI.

3. Authentic sources: the EGDI data providers should consider how they will deal with national authentic sources. If they choose to create pan-European authentic sources, a process should be developed for the creation and recognition of these sources.

4. Security: the EGDI data and service providers should set up a security policy that provides sufficient security, but also maintains as much user-friendliness as possi-

[189] [ENISA 2011].

[190] [ENISA 2011].

[191] J. Camp et al. (2001). “Trust: a collision of paradigms”, *John F. Kennedy School of Government,Harvard University Faculty Research Working Papers Series*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=262179 (accessed on 22/05/2013).

ble. Such a security policy includes an assignment of responsibilities, including decisions on the entities responsible for developing and updating the security policy, maintaining logs for operations, serving as a point of contact for security breaches, performing the compliance audits, etc.

Trust in the services

1. Metadata and quality information: It is recommended that for non-INSPIRE services included in the EGDI, it is examined in how far the metadata requirements of INSPIRE can also be applied. Next, it should be examined in how far the metadata can include information on the fitness for purpose, and which other channels can be used for providing information on the characteristics of the services.
2. Security: The security policy that needs to be developed by the data and service providers in the EGDI needs to pay sufficient attention to services, particularly with regard to access management and guarantees for continuity. In developing this security policy, the role of each party in the EGDI governance structure needs to be clarified.
3. Service level agreements: Service level agreements or terms of service will have to be developed that are feasible for the service providers and that at the same time are sufficient for the users of the EGDI. The EGDI governance structure should consider whether it wants to propose common service levels for all or particular categories of services in the infrastructure.
4. Digital rights management: It should be considered to what extent rights management technology is required and what its exact function should be. Any such technology should be implemented in coordination with the licensing policy that is set up in the EGDI. The GeoRM and GeoREL standards should be used. A support and implementation strategy for implementing GeoRM in the participating organisations should be rolled out.

Trust in the people

1. Identity management system: an appropriate identity management system needs to be set up, that allows for cross-border transactions, and that does not impose too heavy a burden on the users of the system (e.g. often qualified electronic signatures are too 'heavy'). A federated identity management should be considered, and the appropriate software, policies and security for this should be agreed upon. It should be considered whether a third party will be the identity provider, or whether one of the entities in the EGDI will function as the identity provider. Tasks and responsibilities for managing this federated identity management should be allocated in an agreement between all parties in the EGDI that will use the system.
2. Personal data protection: for the processing of personal data from the identity management system, the tasks and responsibilities should be clearly set out and a controller should be assigned. This controller should make sure that
   - It is clearly established which national data protection legislation is applicable;

- A privacy policy is drafted for the EGDI that includes a division of tasks and responsibilities, and organizational and technical measures for the treatment, confidentiality, and security of the personal data. This privacy policy should be disseminated to all partners in the EGDI;
- Consent is obtained in writing from the data subject by using an appropriate standard form for consent;
- The purpose of the processing is legitimate and clearly delineated before the collection of the personal data starts, and the data are not used for any other purpose than the purpose that is communicated to the data subjects. This purpose will be the provision of the data and services, and making sure that only authorised persons get access to these data and services.
- Only the data that are strictly necessary for the purpose can be collected and processed. They have to be destroyed as soon as they are no longer necessary for the purpose.
- The data subjects are appropriately informed about the data processing and about their rights to access, correction and objection.
- The personal data are processed on the territory of a European Member State and not transferred to a country that does not have an adequate level of data protection;
- The competent national Data Protection Authority is notified about the data processing operations.

Moving the EGDI to the cloud

1. Risk assessment: The EGDI governance structure should make a thorough assessment of the advantages and the risks involved, in cooperation with the data and service providers involved in the EGDI. It should compare the services available on the market, and assess in how far they comply with the EGDI's requirements from a technical, organisational and legal perspective.

2. Negotiation: In as far as possible, the EGDI governance structure should negotiate with the cloud service providers so that the requirements of the infrastructure, the data and service providers, and the end users can be met. Points of negotiation could include, among others, exclusion or limitation of liabilities and remedies; service levels, including availability; security and privacy, particularly relating to the Data Protection Directive; lock-in and exit arrangements; providers' ability to change service features unilaterally; intellectual property rights; applicable law and jurisdiction.[192]

[192] [Kuan Hon et al. 2012].

5 References

Ahmed, S. (2010). “Data portability: key to cloud portability”, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1712565 (accessed on 22/05/2013)

Aslesen, L. et al. (2010). “D4.4. Best practice for a licensing policy (including pricing and geo rights management)”, *ESDIN project report*, http://www.esdin.eu/sites/esdin.eu/files/D%204.4%20Final%20Licensing%20policy%20guidelines.pdf (accessed on 23/05/2013)

Article 29 Working Party (2010). *Opinion 1/2010 on the concepts of "controller" and "processor". Opinion 169*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (accessed on 22/05/2013)

Balboni, P.(2010). “Data protection and data security issues related to cloud computing in the EU”, *Tilburg University Legal Studies Working Paper Series*, http://ssrn.com/abstract=1661437 (accessed on 22/05/2013)

Bishr, M. et al. (2007). “GeoDRM: Towards digital management of intellectual property rights for spatial data infrastructures” in H. Onsrud (ed.), *Research and Theory in Advancing Spatial Data Infrastructure Concepts*, Redlands: ESRI, 245-260

Boin, A. and Hunter, G. (2007). “What Communicates Quality to the Spatial Data Consumer?”, *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences* 34 (XXX), http://itc.nl/external/ISSDQ2007/proceedings/Session%205%20Dissemination%20and%20Fitness%20for%20Use/Boin_paper%5B1%5D.pdf (accessed on 22/05/2013)

Camp, J. et al. (2001). “Trust: a collision of paradigms”, *John F. Kennedy School of Government,Harvard University Faculty Research Working Papers Series*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=262179 (accessed on 22/05/2013)

Caufmann, C. (2005). *De verbindende eenzijdige belofte*. Antwerpen: Intersentia, 952 p

Cohen, M. (1933). “The Basis of Contract”, *Harvard Law Review* 46(4), 578-580

Council of Europe (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*, http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (accessed on 22/05/2013)

Cronin, K. (2010). “Best practices and the state of information security”, *Chicago-Kent Law Review* 84, 811-819

Devillers, R. et al. (2002). “Spatial Data Quality: From Metadata to Quality Indicators and Contextual End-User Manual”, *OEEPE/ISPRS Joint Workshop on Spatial Data Quality Management*, 45-55, http://www.researchgate.net/publication/228597904_Spatial_data_quality_From_metadata_to_quality_indicators_and_contextual_end-user_manual/file/d912f50b7c95e4c6c2.pdf

Devillers, R. et al. (2007). “Towards Spatial Data Quality Information Analysis Tools for Experts Assessing the Fitness for Use of Spatial Data”, *International Journal of Geographical Information Science*, 21(3), 261-282

Dumortier, J. et al. (2011). “D.7.1 Legal Requirements for Trust in the IoT”, *uTRUSTit project report*, http://www.utrustit.eu/uploads/media/utrustit/uTRUSTit_D7.1_Legal_Requirements_for_Trust_in_the_IoT_final.pdf (accessed on 22/05/2013)

Dumortier, J. and Vandezande, N. (2012). “Trust in the proposed EU regulation on trust services?”, *Computer Law & Security Review* 28(5), 568-576

Dunne, M. (2008). “Eight significant points in technology outsourcing and remote hosting contracts”, N*ew Jersey Lawyer* 255, 19-22

ENISA (2009). Cloud computing. Benefits, risks and recommendations for information security, http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment (accessed on 22/05/2013)

ENISA (2011). *Mapping security services to authentication levels. Reflecting on STORK QAA levels*, http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/map-auth-lev/at_download/fullReport (accessed on 22/05/2013)

European Commission (2008). Regulation 1205/2008 of 3 December 2008 implementing Directive 2007/2/EC of the European Parliament and of the Council as regards metadata, *OJ L* 326, 4 December 2008, 12-30

European Commission (2010). *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A digital agenda for Europe*, COM (2010) 245 final

European Commission (2012). *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the potential of cloud computing in Europe*, COM(2012) 529 final

European Commission (2012). *Commission proposal for a regulation of the European Parliament and of the Council of 4 June 2012 on electronic identification and trust services for electronic transactions in the internal market*, COM(2012) 238 final

European Commission (2012). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, COM (2012), 11 final

European Parliament and Council (1995). Directive 95/46/EC 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, *OJ L* 281, 23 November 1995, 31-50

European Parliament and Council (1999). Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures (E-signature Directive), *OJ L* 13, 12-20

European Parliament and Council (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), *OJ L* 201, 31 July 2002, 37-47

European Parliament and Council (2006). Directive of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ L* 105, 13 April 2006, 54-63

European Parliament and Council (2007). Directive 2007/2/EC of of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), *OJ L* 108, 25 April 2007, 1-14

European Parliament, Council and European Commission (2010). Charter of Fundamental Rights of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF (accessed on 23/05/2013).

Garon, J. (2011). "Navigating through the Cloud – Legal and Regulatory Management for Software as a Service", *NKU Chase Law & Informatics Institute Working Papers Series*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2025246 (accessed on 22/05/2013)

Joint, A. and Baker, E. (2011). "Knowing the past to understand the present - issues in the contracting for cloud based services", *Computer Law and Security Review* 27(4), 407-415

Kuan Hon, W. et al. (2011). "Who is responsible for personal data in cloud computing? – The cloud of unknowing part 2", *International Data Privacy Law* 2(1), 1-18, http://idpl.oxfordjournals.org/content/2/1/3.full (accessed on 22/05/2013)

Kuan Hon, W. et al. (2012). "Negotiating cloud contracts: looking at clouds from both sides now", *Stanford Technology Law Review* 16, 79-128

Li, D. et et al. (2012). "Spatial data quality and beyond", *International Journal of Geographic Information Science*, 26(12), 2277-2290

Martin, T. (2010). "Hey! You ! Get off my cloud: defining and protecting the metes and bounds of privacy, security, and property in cloud computing", *Journal of the Patent and Trademark Office Society* 92, 283-314

May, C. (2013). "Seeing into the Cloud: How to Mitigate Potential Ethical and Security Issues, *Federal Lawyer* 60, 69-76

Mell, P. and Grance, T. (2011), *The NIST definition of cloud computing, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf* (accessed on 22/05/2013)

Mik, E. (2012). "Mistaken identity, identity theft and problems of remote authentication in e-commerce", *Computer Law & Security Review* 28(4), 396-402

Morgan, R. et al. (2004). "Federated security: the Shibboleth approach". *Educause Quarterly* 4, 12-17

OECD (2002). *Guidelines for the security of information systems and networks: towards a culture of security*, http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm (accessed on 24/05/2013)

Rajabifard, A. et al. (2009). "SDI and Metadata Entry and Updating Tools" in B. Van Loenen et al. (ed.). *SDI Convergence. Research, Emerging Trends, and Critical Assessment*, Delft: Netherlands Geodetic Commission, 121-136

RAND (2010). *The Cloud: Understanding the Security, Privacy and Trust Challenges*, http://www.rand.org/pubs/technical_reports/TR933.html (accessed on 22/05/2013)

Scheckler, V. et al. (s.d.). *Liberty Alliance Contractual Framework Outline for Circles of Trust*, http://www.projectliberty.org/liberty/content/download/2962/19808/file/Liberty%20Legal%20Frameworks.pdf (accessed on 22/05/2013)

Smedinghoff, T. (2007). "It's all about trust: the expanding scope of security obligations in global privacy and e-transactions law", *Michigan State Journal of International Law* 16(1), 1-47, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1100712 (accessed on 23/05/2013)

Smedinghoff, T. (2009). "Federated Identity Management: Balancing Privacy Rights, Liability Risks, and the Duty to Authenticate", http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471599 (accessed on 23/05/2013)

Soma, J. et al. (2011). "Chasing the clouds without getting drenched: a call for fair practices in cloud computing services", Journal of Technology Law & Policy 16, 193-227

Spyrelli, C. (2002). "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication", *Journal of Information Law and Technology* 2(2), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/?textOnly=false (accessed on 23/05/2013)

Steinauer, D. et al. (1997). "Trust and traceability in electronic commerce", *StandardView* 5(3), 118-124

Sultan, F. et al. (2002). "Determinants and Role of Trust in E-business. A Large Scale Empirical Study", *MIT Sloan School of Management Working Paper*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=380404 (accessed on 22/05/2013)

Taylor, M. and Matteucci, M. (2010). "Cloud computing", *Computer and Telecommunications Law Review*, 57-59

Van Alsenoy, B. et al. (2011). "D3.1. Legal Provisions for Deploying INDI services", *GINI Support Action project report*, http://www.gini-sa.eu/images/stories/2011.11.06_GINI_D3.1_Legal%20Provisions%20for%20Deploying%20INDI%20Services_FINAL.pdf (accessed on 22/05/2013)

Wayne, L. (2005). "Metadata in Action. Expanding the Utility of Geospatial Metadata*", GIS Planet* June 2005, 1-6