GLOBAL IDENTITY NETWORKING OF INDIVIDUALS

Legal Provisions for deploying INDI Services

Version 1.0

Project Name	GLOBAL IDENTITY NETWORKING OF INDIVIDUALS
Work Package	WP3 – The Legal and Regulatory dimension of the INDI Domain
Activity	A3.1: Curent ID-related legal framework A3.2: Legal provisions for deploying INDI services
Editors	Brendan Van Alsenoy (ICRI, K.U.Leuven)
Date of Initial Creation	23.02.2011
Date of Last Change	19.06.2011
Status	[ ] Draft [ ] Internal Commenting [x] Release
CM Path	...

Further Document Information

Authors	Brendan Van Alsenoy (ICRI, K.U.Leuven) (ed.) Niels Vandezande (ICRI, K.U.Leuven) Dr. Katleen Janssen (ICRI, K.U.Leuven) Aleksandra Kuczerawy (ICRI, K.U.Leuven) Els Kindt (ICRI, K.U.Leuven) Prof. Dr. Jos Dumortier (ICRI, K.U.Leuven) Herbert Leitold (TUG) Bernd Zwattendorfer (TUG) Ioannis Krontiris (GUF)
Base Documents	

Change History

Modification			Affected Chapters	Motivation / Description	Author	State
No.	Date	Version				
1	23-02-2011	0.1	All	Initial creation	BVA, NV	Draft
2		0.2	4	Data protection	BVA, EK	Draft
3	21-03-2011	0.3	5	Re-use of PSI	KJ, NV BVA	Draft
4	05-04-2011	0.4	6	E-Commerce	AK, BVA, NV	Draft
5	23-05-2011	0.5	7	E-Signatures	BVA, NV	Draft
6	22-05-2011	0.6	4	eID interoperability barriers	HL, BZ	Draft
7	12-06-2011	0.7	4	Data Minimization techniques	IK	Draft
8	17-06-	0.8	All	Integration feedback	BVA	Draft

	2011			internal reviewer 1 (TA)		
9	19-06-2011	0.9	All	Internal reviewer 2 (SG)	BVA	Draft
10	19-06-2011	1.0				Release

Audit and Quality Assurance History

No.	Date	Version	Remarks	Auditor	State
1					

Table of Contents

Executive Summary

GINI-SA aims to analyse how a *Personalized Identity Management (PIM) ecosystem* can be created where individuals can manage their own digital identities and control the exchange of their identity information. The objective of this deliverable is to analyse the main legal requirements affecting the development of a PIM ecosystem and the provisioning of INDI Services. While in the context of GINI considerable emphasis will be placed on privacy and data protection regulation, this deliverable also elaborates upon other areas of EU regulation which may impact the development of the PIM ecosystem. In total, four areas of EU regulation are investigated, namely:

- Data protection and privacy;
- Re-use of public sector information;
- e-Commerce; and
- Electronic signatures.

The analysis of each of these areas of regulation begins by providing a high-level description of the regulatory framework that is currently in place. Next, the main implications of these regulations for the development and deployment of INDI Services are elaborated. The key objective of this exercise is to identify relevant legal requirements and articulate potential barriers and gaps for the development of INDI Services on either a national or pan-European level.

The findings of this deliverable will serve as input to GINI D3.2 ('A regulatory framework for INDI operators'). This deliverable will outline areas in which further regulation may be needed to create a legal framework which is sufficiently conducive to the development of privacy enhancing identity management services. The findings of both these deliverables will also serve as input to GINI D5.1 (Research and implementation roadmap) and GINI D5.2 (White Paper).

1 Introduction and scope

In today's information society, identity data can be found in practically every organization. This information is maintained and managed for a wide variety of purposes (e.g., customer relations management, HR management, payroll administration, public service delivery). Identity data is also increasingly exchanged across organizational boundaries. These exchanges are similarly driven by a multiplicity of purposes (e.g., outsourcing, joint ventures, integrated service delivery, profiling). As the information society continues to develop, we may expect such exchanges to increase.

As the organizations providing and receiving identity information are typically (in one way or another) 'consumers' of this information, the exchange of identity data and other personal information is currently organized in a very 'service provider-centric' (or 'vendor-centric') fashion. In addition, many identity management solutions are tailored to the specific needs of individual organizations or a specific context of use, thus impeding their re-use in other settings.

GINI-SA aims to analyse how a *Personalized Identity Management (PIM) ecosystem* can be created where individuals can manage their own digital identities and control the exchange of their identity information. In recent years, much research has been performed on the topic of user-centric identity management.[1] The main aim of this research was usually technical feasibility rather than legal realization. In addition, much of the legal research in this area has focused mainly on compliance aspects. Only limited research has been conducted to identify the potential legal barriers towards the development and actual deployment of user-centric identity management services, be it on a national or pan-European level. Similarly, only limited research has been performed to determine whether additional regulation may be needed in order to enable the development of a PIM ecosystem.

The objective of this deliverable (D3.1) is not only to identify relevant legal requirements, but also to articulate potential barriers and gaps. Our area of focus will be those regulatory initiatives which govern (or otherwise impact) the provisioning and use of digital identities. In a first step, we will start by identifying areas of relevant EU regulation. While in the context of GINI considerable emphasis will be placed on privacy and data protection regulation, we shall also elaborate upon other areas of EU regulation which may impact the development of the PIM ecosystem. For each of these we will begin by providing a high-level description of the regulatory framework that is currently in place. Next, we will elaborate upon the main implications of these regulations for the development and deployment of INDI Services. The key objective of this exercise is to identify relevant legal requirements and articulate potential barriers and gaps.

As Directives are the main EU legal instruments in this field, differences in policies across EU Member States are still a reality. A detailed overview and comparative analysis of the regulation of all EU Member States in these areas is beyond the scope of this document. For certain areas, a comprehensive comparative analysis has already taken place in the context of other projects or programmes, such as IDABC[2], STORK[3] and PEPPOL[4]. It is not our intention to repeat the same

[1] See e.g. PRIME (https://www.prime-project.eu); PrimeLife (http://www.primelife.eu) and PICOS (http://www.picos-project.eu).
[2] http://ec.europa.eu/idabc/
[3] https://www.eid-stork.eu/
[4] http://www.peppol.eu/

exercise here. Our aim is to identify, building inter alia upon the findings of these projects, the key legal issues and potential barriers to the implementation of user-centric identity management applications and services.

The findings of this deliverable will serve as input to GINI D3.2 ('A regulatory framework for INDI operators'). This deliverable will outline areas in which further regulation may be needed to create a legal framework which is sufficiently conducive to the development of privacy enhancing identity management services. The findings of both these deliverables will also serve as input to GINI D5.1 (Research and implementation roadmap) and GINI D5.2 (White Paper).

2 GINI Vision[5]

2.1 A Personalized Identity Management ecosystem

As indicated in the introduction, GINI aims to analyse how a Personalized Identity Management (PIM) ecosystem can be created where individuals can manage their own digital identities and control the exchange of their identity information. Under the GINI vision, individuals would manage their identities by means of an Individual Digital Identity ('INDI'). An INDI can be described as a self-created and self-managed digital identity, which is verifiable against one or more authoritative data sources. Once created, users would have the ability to link their INDI with authoritative identity data maintained by both public- and private-sector entities. This data (or links thereto) could then be presented by the user towards relying parties. The user might wish to do this in order to meet transactional requirements (e.g., access control conditions set by a relying party) or to improve the perception of her trustworthiness towards others (e.g., when selling a car). The basic assumption is that relying parties will have greater confidence in the attributes asserted by an individual if these attributes are confirmed by an independent entity which is generally perceived as maintaining high-quality information.

One of the most prominent functionalities of an INDI (and the INDI infrastructure in general) is that it allows its user to present information about themselves in a verifiable fashion, i.e. in a manner which provides relying parties with appropriate assurance as to the authenticity of the data that is presented (i.e. that the data originates from the identified source and has not been manipulated during transmission).

Under the GINI vision, the disclosure of personal information requires user authorization (consent) by default. Disclosure may exceptionally occur without the user's consent only in cases mandated by law.

2.2 An operator-based trust model

The PIM ecosystem envisioned by GINI is based on a network of Operators. In order to create and use an INDI, an individual must establish and maintain a relationship with at least one INDI

[5] The conceptualization of the GINI vision has taken place in the context of GINI D1.1 ('The Individualised Digital Identity (INDI) Model: A User-centric Framework of identity management services). It is nevertheless useful to summarize its main elements here as we will be referencing a number of core concepts throughout this deliverable.

Operator. A basic premise of the project is that this (contractual) relationship should be sufficient for attaining access to the whole INDI environment (thereby removing - or at least minimizing - the need for additional one-to-one contracts). The other entities involved in the PIM Ecosystem (Data Sources and Relying Parties) are also expected to establish a relationship with at least one INDI Operator in order to connect to the INDI environment. This Operator does not need to be the same as the Operator of the individual concerned. Rather, a plurality or 'network' of Operators is envisioned. The conceptual model of the PIM Ecosystem envisioned by GINI can be visually represented as follows:

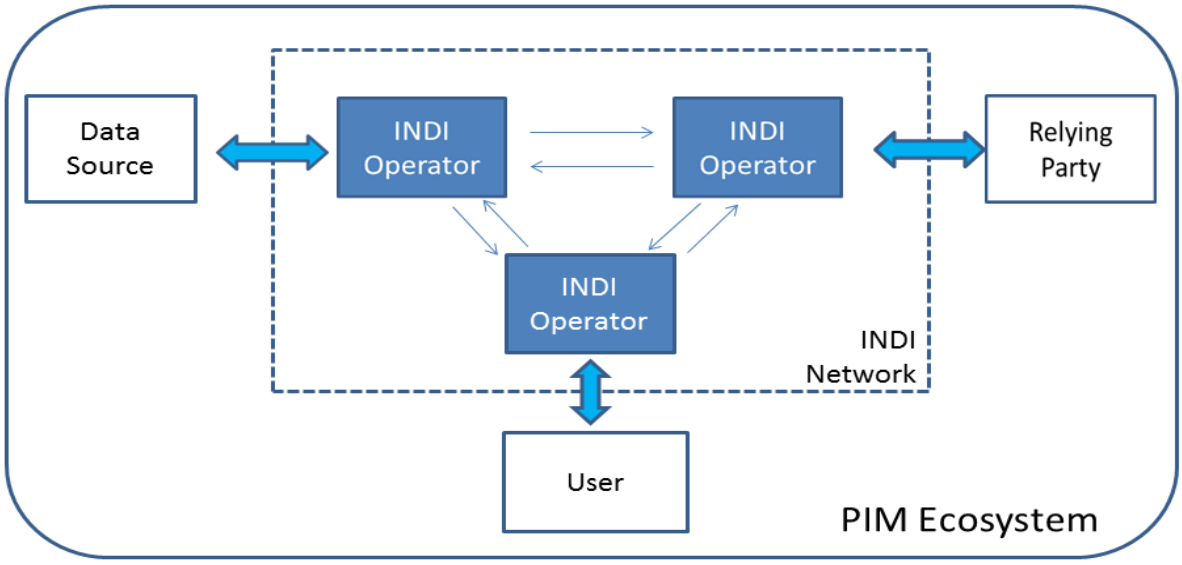

Figure 1 – GINI Conceptual Model

The main role of the INDI Operators is to act as trust anchors. Their services are designed to provide other entities within the PIM Ecosystem with the assurances they need in order to enable the disclosure and reliance upon identity information, even where the parties involved do not have pre-established trust relationships. The main services of an INDI Operator include:

- creating and distributing INDIs and INDI addresses in such a way that they can be used within the INDI environment and presented towards relying parties;
- ensuring that no-one can determine the identity of the INDI user, unless the user voluntarily discloses it or such disclosure is mandated by law;
- obtaining consent from users for the disclosure of their personal information maintained by a data source;
- ensuring the authenticity (i.e. source and integrity) of data presented towards relying parties;
- managing a reference directory (displaying which Data Sources maintain information about users); and
- ensuring technical interoperability among the parties involved in a transaction in the INDI environment.

An INDI Operator in principle does not:

- make any warranties with regard to the reliability of the content of information maintained by a Data Source; nor

- store or aggregate any information exchanged between Users and Relying Parties.

2.3 Relationships among the actors

The purpose of this subsection is to outline the main characteristics of relationships among the actors of the PIM Ecosystem. One of the aims of this outline is to make explicit the trust relationships that exist among the entities interacting through the INDI network. The term 'trust' is used here in a very broad sense, and refers to the 'baseline behavioural expectations' that the actors have towards one and other (thereby making abstraction for the moment as to how this trust relationship is translated technically or legally).[6]

2.3.1 INDI Operator –User

A contractual relationship exists between the INDI Operator and the INDI user which governs the terms of service. Pursuant to these terms of service, the INDI Operator commits to providing its users with the ability to create an INDI which in turn enables them to present verifiable (links to) data about themselves.

This set-up supports a number of assumptions regarding the trust relationship between the INDI operator and the user, the main properties of which can be summarized as follows:

a. The user trusts its INDI Operator to deliver the basic INDI functionality, i.e. to facilitate the disclosure/presentation of information about her maintained in one or more Data Sources for the benefit of Relying Parties. The User relies upon the Operator to interact with these entities (or their agents) in a way which will make the desired data exchange(s) possible.

b. The User trusts its INDI Operator that it will not facilitate or otherwise enable the disclosure of here personal information towards other entities without her consent (unless required by a legal obligation to which INDI Operator is subject).

c. The User trusts its INDI Operator to adopt appropriate measures to authenticate (information coming from) both Data Sources and Relying Parties.

d. The INDI Operator relies upon the User to adhere to its terms of service for end-users and to only authorize disclosure of information that match the user's own intent.[7]

e. The INDI Operator relies upon the User to protect the credentials she uses to access her INDI (which may include credentials issued by the Operator) and to take appropriate measures in case they are compromised (e.g., revocation, renewal). The User similarly relies upon the Operator to implement appropriate technical and organizational measures to prevent impersonation of the Operator (mutual authentication).

[6] See also S. Murrow and E. Maler (eds.), *UMA Trust Model* (v.2), Kantara Initiative, 24 February 2011, available at http://kantarainitiative.org.

[7] See also S. Murrow and E. Maler, *o.c.*, TR-2a and TR-4.

2.3.2 INDI Operator –Relying Party

A contractual relationship exists between the INDI Operator and the relying party which governs the terms of service. The operator-based trust model implies that the Relying Party will in principle only trust a particular claim made by a user on the condition that the necessary interventions have been made by the INDI Operator.[8]

The main properties of the trust relationship between the INDI operator and the Relying Party can be summarized as follows:

a. The Operator trusts the Relying Party to adhere to its terms of service for relying parties.

b. The Operator trusts the Relying Party to protect the credentials she uses to authenticate herself towards the Operator (which may include credentials issued by the Operator) and to take appropriate measures in case they are compromised (e.g., revocation, renewal). The Relying Party similarly relies upon the Operator to implement appropriate technical and organizational measures to prevent impersonation of the Operator (mutual authentication).

c. The Relying Party trusts the Operator to only request (corroborative) information about her where this is necessary to complete the transaction (e.g. in order to meet the user's authorization constraints/policies).[9]

d. The Relying Party trusts the Operator to ensure that the data it receives is authentic, i.e. emanates from the identified source and has not been subject to manipulation.

2.3.3 INDI Operator(s) –Data Source

A Data Source will also connect to the INDI Network by means of a contract with one or more INDI Operators of its choice. This contract will in first instance establish the conditions under which (and mechanisms through which) the Data Source will make available (links to) data to either the User or the Operator.

The main properties of trust relationship between the INDI Operator and the Data Source can be summarized as follows:

a. The Data Source relies upon its Operator to provide (or at least identify) the appropriate technical interface to process the user-authorized disclosure of personal information.

b. The Data Source relies upon its Operator to provide accurate information with regard to the authorizations granted by the User (e.g., their scope, validity period etc.).[10]

c. The Operator relies upon the Data Source to adhere to its terms of service for Data Sources.

d. The Operator relies upon the Data Source to protect the credentials she uses to authenticate herself towards the Operator (which may include credentials issued by the Operator) and to

[8] Of course it remains possible that the Relying Party also trusts one or more credentials directly, without intervention of an INDI Operator. However, this relationship then lies beyond the boundaries of the INDI Network.

[9] S. Murrow and E. Maler, *o.c.*, TR-12.

[10] See also S. Murrow and E. Maler, *o.c.*,TR-7c.

take appropriate measures in case they are compromised (e.g., revocation, renewal). The Data Source similarly relies upon the Operator to implement appropriate technical and organizational measures to prevent impersonation of the Operator (mutual authentication).

e. The Operator relies upon the Data Source to respect the boundaries of the authorizations granted by the User (e.g. not to make available more attributes than the User has intended).[11]

2.3.4 Data source –Relying Party

The GINI conceptual model does not assume a direct relationship among these actors. While it does not exclude the possibility of such a relationship existing, it is equally possible that their relationship is mediated entirely through the INDI infrastructure.

The main properties of trust relationship between Data Source – Relying Party are:

a. The Relying Party will need to be able to trust that the information maintained by the Data Source is accurate and up to date, or at least that the Data Source abides by its stated practices.

b. The Data Source will require assurance of the legitimacy of data disclosure in one way or another; particularly where the envisaged disclosure cannot be deemed 'compatible' with the purposes for which the Data Source is currently processing the data.[12]

2.3.5 Data Source – INDI User

The GINI conceptual model does not explicitly require a direct relationship among these actors. However, in many instances these actors will have (had) a direct relationship with one and other which has not been (previously) mediated by the INDI Network. The nature of this relationship is in principle context-specific and can take on a wide variety of forms (e.g. governmental agency – citizen; SNS provider – SNS user).

The main properties of trust relationship between Data Source – INDI User are:

a. The User relies upon the Data Source to interact with an INDI Operator and to accept her own INDI Operator as her proxy (for the capturing of her consent/authorization).

b. The User will need to be able trust the Data Source to only make accurate representations about her when divulging information towards other parties.

2.3.6 Relying Party – INDI User

The GINI conceptual model does not explicitly require a direct contractual relationship among these actors. The disclosure of personal information by the INDI User to the Relying Party shall be mediated by the INDI Network. However, given the fact that the INDI User voluntarily discloses certain information about herself to the Relying Party it may be assumed that these actors will additionally establish direct relationship with one and other outside the context of the

[11] *Ibid*, TR-8c.
[12] See also *infra*; section 4.6.1.

INDI Network. The nature of this relationship will in principle be context- or even transaction-specific (e.g. service provisioning, job application). It is important to note that a Relying Party may be both an organization as well as a natural person connecting to the INDI environment for personal purposes. In the latter case the relationship between may also be characterized as relationship among INDI Users, which is also mediated by their respective INDI Operators.

In both scenarios the relationship among INDI User and the Relying Party will depend mainly on the context of their interactions and/or the nature of their transaction. However, the mediation by the respective INDI Operators is bound to exercise a key role when the trust relationship between the INDI User and Relying Party is established.

3 Overview of relevant areas of EU regulation

In the context of this deliverable, the following areas of EU regulation will be investigated:

- Data protection and privacy;
- Re-use of public sector information;
- E-Commerce; and
- Electronic signatures.

Each of these areas of regulation will be elaborated in more detail in the following chapters of this document. As indicated in the introduction, our aim is to not only identify legal requirements affecting the development of a PIM ecosystem and the provisioning of INDI Services, but also to identify potential legal barriers and other issues which will require further consideration.

4 Data protection

4.1 Directive 95/46/EC

The main legal instrument on data protection in the EU is Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[13] This Directive – implemented into national law across the EEA – formulates the basic principles and rights of data subjects in relation to the processing of their personal data.

Directive 95/46/EC was adopted, as its title suggests, to serve a dual purpose. In first instance it sought to facilitate cross-border flows of data within the Community by harmonizing the national data protection legislation of the Member States (which might otherwise present obstacles to the free movement of personal data within the internal market).[14] At the same time, Directive 95/46/EC also sought to ensure a high level of data protection within the Community.[15]

The aim of this chapter is to discuss how the current data protection framework might impact the development of a Personalized Identity Management ecosystem in general, and the development of INDI services in particular. We will start by outlining the scope of this Directive, after which we will provide an overview of the main requirements and implications of this Directive. During this discussion we will point out areas in which the regulatory framework might be challenged by certain approaches and practices, but also attempt to provide recommendations as to how these challenges might be addressed. We will also pay particular attention to barriers and gaps resulting from the current framework.

[13] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Official Journal of the European Union, n° L 281, 23 November 1995, p. 31–50. Hereafter also referred to as 'Directive 95/46/EC' or simply 'the Directive'.

[14] See in particular recital (9) of Directive 95/46/EC.

[15] See in particular recital (10) of Directive 95/46/EC.

4.2 Scope

Directive 95/46/EC applies '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' (art. 3, 1). The scope of the Directive covers all automated processing of personal data, save for the areas excluded by art. 3, 2 of the Directive, namely the processing of personal data:

- - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law; and
- - by a natural person in the course of a purely personal or household activity.

The provisioning of INDI services will fall within the ambit of the ambit of this Directive. Identity data and personal attributes are considered personal data as long as they relate to an identifiable person. As noted by the Article 29 Working Party: 'data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated'.[16] Seeing as the very purpose of INDI Services is to allow individuals to present information about themselves (in a verifiable fashion), they will by definition involve personal data processing.

4.3 Definition of actors, roles and responsibilities

4.3.1 Qualification of actors[17]

Under the framework of Directive 95/46/EC, there are at least two actors implicated in any personal data processing operation: a controller and a data subject. A data subject is essentially any individual to whom the information relates, provided that he or she is identified or sufficiently identifiable (see art. 2, a).[18] The controller is defined by the Directive as the entity who alone, or jointly with others, determines the '*purposes and means*' of the processing (art. 2, d). A third important actor identified by the Directive is the 'processor'.[19] A 'processor' is defined as an entity who processes personal data *on behalf* of the data controller (art. 2, e).

Both the controller and the processor concepts are essential to the regulatory scheme of Directive 95/46/EC. Together, these concepts provide the very basis upon which responsibility

[16] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data', WP 136, 20 June 2007, p. 10.

[17] This subsection is comprised primarily of extracts of a forthcoming publication: B. Van Alsenoy, 'Allocating responsibility among controllers, processors "and everything in between": a preliminary analysis of structural issues underlying the definition of roles and responsibilities in Directive 95/46/EC', submitted to Computer Law and Security Review.

[18] B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, 'Social networks and web 2.0: are users also bound by data protection regulations?', *Identity in the information society*, Vol. 2, n°1, October 2009, 68 (available at http://www.springerlink.com/content/u11161037506t68n/fulltext.pdf, last accessed 24 November 2010).

[19] Directive 95/46/EC also identifies 2 other types of actors, namely 'recipients' and 'third parties'. However, seeing as neither qualification triggers any specific obligations they are not discussed separately in the context of this deliverable.

for compliance with the substantive provisions of the Directive is allocated. The primary responsibility for compliance is assigned to the controller, as is the corresponding liability exposure. Processors on the other hand, who merely execute processing operations at the direction of a controller, shall as a rule only be indirectly accountable for compliance obligations.[20] Given the fundamental importance of the qualification as either a controller or a processor, it is crucial to be able to determine in which capacity an entity is performing a particular processing operation.[21] Despite this reality, technological developments since the enactment of the Directive have made it increasingly difficult to apply the distinction between 'data controller' and 'data processor' in practice.[22]

GINI envisages an ecosystem in which multiple actors collaborate in order to enable individual users to manage the disclosure of their personal information. The nature of the relationship between these actors under data protection law can take on many different forms: a controller-processor relationship, a controller-to-controller relationship, a relationship of joint control, etc.[23] It is important to realize that the legal qualification of a 'controller' is not dependent on whether or not an entity has operational control over the data. For instance, it could be that the entity that legally qualifies as the controller does not store any of the information himself, but relies entirely on a hosting service outside its organization that makes this information available upon its request. It is also possible that it has direct access to the information, but that the enforcement of authorization policies and privilege management is organized by yet another entity. Thus the Directive has introduced the possibility of 'dualism' between control from a legal perspective (which brings about the responsibilities of a 'controller') on the one hand, and control from a practical ('operational') perspective on the other hand (the ability to enforce access control policies, the ability to delete, etc.). It is possible that in practice both notions of control coincide, but it also possible that there is only a partial overlap; or even that a dichotomy exists between them. As a result certain obligations incumbent upon the controller may in practice more easily be observed by an entity which does not qualify as the controller (or at least not as the sole controller) for the data processing.

The Article 29 Working Party has acknowledged this reality and emphasized that, even where the controller's obligations may in practice be more easily fulfilled by other parties (e.g., if those parties have a more direct relationship with the data subject), it is the controller that remains 'ultimately responsible for its obligations and liable for any breach to them'.[24] Where multiple parties jointly exercise control, the Working Party has stated that these entities have a certain degree of flexibility when allocating responsibility amongst each other, as long as they ensure full compliance.[25] More specifically, the bottom line should be that

[20] See also J. Alhadeff and B. Van Alsenoy (eds.), 'Deliverable 6.2 Contractual Framework', *Trusted Architecture for Securely Shared Services (TAS³)*, third iteration, 34, available at www.tas3.eu.

[21] B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, 68.

[22] Kuner, C., *European Data Protection Law – Corporate Compliance and Regulation*, second edition, Oxford University Press, New York, 2007, p. 71–72.

[23] Olsen and Mahler have developed an interesting visual representation of the different degrees of collaboration among (co-)controllers. See T. Olsen and T. Mahler, 'Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II', *Computer, Law & Security Review* 2007n Vol. 23, n° 5, 419-420.

[24] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller and "processor"', WP169, 16 February 2010, p. 22 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf. Hereafter referred to as "Opinion 1/2010".

[25] Opinion 1/2010, *l.c.*, 24.

> *'[…] even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules are clearly allocated, in order to avoid that the protection of personal data is reduced or that a "negative conflict of competence" and loopholes arise whereby some obligations or rights stemming from the Directive are not ensured by any of the parties'.*[26]

While there is a certain degree of flexibility in the distribution of tasks and responsibilities, each actor's role must still be accounted for (in the sense that each actor's obligations under data protection law must be taken into account).[27] The INDI services envisioned by GINI can be realized in a variety of ways. Although there has been a high-level conceptualization of the actors and their operational role, the actual implementation will vary in practice. It is however already clear that each INDI service will involve a plurality of actors, who will each influence the processing required to realize these services to a greater or lesser extent. Under the current model, any release of personal data concerning an INDI User can easily involve up to five different entities (other than the INDI user to whom the information relates)[28]: at least one Data Source, three INDI Operators (one for the Data Source, one for the User and one for the Relying Party) and (at least) one Relying Party to whom the data shall be made available. Each of these actors may be acting as a controller in respect of one or more of the processing operations that are needed realize the overall functionality, namely the disclosure (or making available) of verifiable information about an INDI User to a Relying Party. It may be expected that both the provider (Data Source) and recipient (Relying Party) of the data shall in principle each act as a data controller in relation to their own processing operations.[29] The storage of data by a Data Source shall in principle be the result of its own business purpose(s) (in the case of private entities) or public mission (in the case of governmental entities).[30] Similarly, the Relying Party to whom the data is made available will be collecting these data for its own purposes. The INDI Operators will fulfill primarily an intermediary function, which will require at least a determination of the means to enable the exchange of data. The extent to which each of these actors are considered to act as (co)controllers towards the various processing operations needed to deliver the overall functionality of INDI services will depend mainly on how they choose to structure their collaboration and the factual influence of each actor towards each operation.

4.3.2 Users as data controllers?

One of the primary aims of GINI is to enable individuals to manage the exchange of their own identity information. They shall in principle decide which information shall be released to which entity in which context. This raises the question as to whether or not the users of INDI Services might be considered as (co-)controllers towards the processing of their own personal data. After all, the determination of which data shall be processed and who will have access to them are

[26] Opinion 1/2010, *l.c.*, 22.

[27] J. Alhadeff and B. Van Alsenoy (eds.), 'Deliverable 6.2 Contractual Framework', *l.c.*, 41. The contractual designation of an entity as either a controller or processor may be indicative of their actual qualification, but is by no means decisive seeing as these roles and their implications are mandatorily defined.

[28] Cf. *supra*; figure 1.

[29] For the purpose of our current discussion we make abstraction of the fact that the recipient might also be another INDI User who may in certain instances benefit from the personal use exemption.

[30] We currently also make abstraction of the fact that an INDI Register might be a processor hosting the information on behalf of a controller. Where this is the case, however, the former is bound to only process the data pursuant to the instructions issued by the controller (see art. 17, 3 Directive 95/46/EC).

considered to be 'essential elements' of the processing which are traditionally and inherently reserved to the determination of the controller.[31]

There are essentially two arguments which can be made against the suggestion that the users of INDI services might act as data controllers towards the processing of their own personal data. First, this interpretation cannot be reconciled with the regulatory scheme of Directive 95/46/EC. This scheme is predicated on the notion that the data controller is an entity other than the data subject him- or herself. An individual person might act as a controller of personal data relating to others[32], but not of his or her own personal data. Accepting that the data subject could act as a controller of the processing of his own personal data would have rather absurd implications: the data subject would have to obtain consent from him- or herself, provide him- or herself with notice, etc.[33] Second, the fact that the data subject authorizes the disclosure of personal information within a certain context merely signifies his or her agreement towards processing. This does not exclude the presence of another entity who determines the 'purposes and means' for the processing of these data, on the contrary. The consent of the data subject may provide a legitimate basis for the processing (cf. *infra*), but this fact alone does not alter the role qualification of the actors involved. Even where the individual has the ability to 'control' the release of his or her personal data (and might even decide the medium that is used), this does not negate the responsibilities of the collectors or handlers of the individual's data.[34]

This said, it is also clear that the current definition of actors and roles established by the Directive is increasingly challenged due to the 'digital emancipation' of data subjects. When the first data protection legislations emerged, large-scale data processing used to be the prerogative of governments, universities, or companies with substantial financial resources. Technological and societal developments since then have made it possible for almost anybody to engage in personal data processing which may significantly affect the privacy interests of both themselves and others. The extent to which the service providers who enable such processing act as (co)controllers is not always clear. This 'democratization of control' calls into question, at least to a certain extent, the premises upon which the definition of roles and responsibilities in Directive 95/46/EC was based.

4.3.3 Allocation of responsibilities

Ensuring compliance with Directive 95/46/EC requires more than just distinguishing among controllers, processors and third parties. Many of the substantive requirements set forth by the

[31] See Opinion 1/2010, *l.c.*, 14.

[32] See European Court of Justice , C-101/01, Bodil Lindqvist, 6 November 2003, O.J. 10 January 2004, C 7/3-4, available at http://curia.europa.eu. See also B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, 69-70; Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking', WP163, 12 June 2009, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf; European Network and Information Security Agency (ENISA), 'Online as soon as it happens', February 2010, p. 33-34, available at http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens.

[33] Alternatively, one could argue that such processing would be exempted from the application of the Directive under art. 3, 2 (exemption of processing carried out in the course of a purely personal or household activity) (see references in previous footnote). However, this finding would not undercut the argument that the allocation of responsibilities under the Directive is structured implies that the data subject and the controller are separate entities.

[34] In other words, the 'control' exercised by the user of INDI services should be considered primarily as a more granular articulation of their consent.

Directive imply the need for organizational and technical measures which are not enumerated in the Directive, but which are nevertheless necessary in order to ensure compliance. How these safeguards are to be implemented will depend more on the operational role of each actor than on their legal qualification. While the operational implications of the substantive requirements of the Directive will be discussed throughout this deliverable, we can already identify a number of tasks which need to be considered. The following is a (by no means exhaustive) list of tasks and responsibilities which will most likely need to be allocated in the context of INDI Services[35]:

- collection, registration and management of data subject consent;
- identification, authentication and authorization of users;
- maintenance of logs for the different processing operations that take place;
- trusted (third) party services (e.g., attribute certification, identifier conversion);
- updating of technical policy information in accordance with permissions granted by data subject and legal developments;
- accommodation of data subject rights such as the right of access and correction; and
- oversight; including regular verification of compliance, redress and point-of-contact in the event of a security breach (audit).

4.4 *Legitimacy of processing*

The EU Data Protection Directive 95/46/EC restricts the instances in which the processing of personal data may take place. In particular, articles 7 and 8 of this Directive enumerate several legal grounds, of which at least one must be present in order for the processing of personal data to be legitimate (principle of legitimacy of processing).[36]

4.4.1 Consent as the default basis for processing

As already indicated, one of the primary aims of GINI is to enable individuals to manage the exchange of their identity information. Disclosure of personal information within this context shall therefore in first instance be based on the consent of data subjects.

In order for consent to provide a legitimate basis for the processing, several requirements must be met. Specifically, in order to be valid, the consent must be[37]:

- unambiguous: the consent must be unequivocal, which means that it may only be understood as the data subject's agreement that personal data relating to him will be processed[38];
- specific: The consent of the data subject must also relate to a well-defined, concrete situation, in which the processing of his personal data is envisaged.[39] It would be

[35] See also FIDIS 16.3, *o.c.*, 17.

[36] Whether one of the grounds of either art. 7 or art. 8 may be used depends on the nature of the personal data. Art. 7 relates to 'normal' personal data, whereas art. 8 outlines the possible legitimacy grounds for 'special categories of data' (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life).

[37] See art. 2, h *juncto* 7, a of the Directive.

[38] D. De Bot, *Verwerking van Persoonsgegevens* ['Processing of Personal Data'], Kluwer, Antwerpen, 2001, p. 129.

[39] Article 29 Data Protection Working Party, 'Working Document on the processing of personal data relating to health in electronic health records (EHR)', WP 131, 15 February 2007, p. 8, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf.

insufficient for the data subject to have consented to "open-ended" processing of his personal data, without having any idea of the exact purposes and modes of processing;

- freely given: this means that the consent must be a voluntary decision, by an individual in possession of all his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other[40]; and
- informed: the consent must be based upon an appreciation and understanding of the facts and implications surrounding the processing.[41] In order to meet this imperative, it is necessary that the controller provides the data subject with accurate and full information of all relevant issues, such as the nature of the data processed, purposes of the processing, the recipients of possible transfers, etc.[42]

Where special categories of data are concerned (e.g., data revealing racial or ethnic origin or data concerning health or sex life – also referred to as 'sensitive data'), a slightly different regime is in place. Specifically, art. 8 of the Directive does not require that the consent must be 'unambiguous', but instead stipulates that such consent must be 'explicit'. Article 29, Working Party, has stated that 'opt-out' solutions will not meet the requirement of being 'explicit'. The data subject's declaration of intent, explicitness must relate, in particular, to the sensitivity of the data.[43] The other requirements for valid consent (specific, freely given, informed) are the same as for 'non-sensitive' data.

4.4.2 Implications

As consent is expected to act as the default basis upon which processing shall be legitimized, at least one of the actors involved in the data processing (or an agent thereof), must be charged with the collection and registration of such consent. This actor must of course ensure that the legal requirements towards consent identified in the previous subsection are satisfied. As indicated, these requirements vary slightly depending on the nature of the personal data concerned.

Which entity should be charged with obtaining consent for which processing operations shall depend in part on the manner in which the communication among the various actors is organized? The GINI vision assumes the presence of multiple INDI Operators who mediate trust among the different actors involved. One of the underlying objectives of the GINI conceptual model[44] is to remove (or at least minimize) the need for bilateral negotiation and/or communication among the different actors when making use of INDI Services. The INDI Operator with whom the INDI User has a direct contractual relationship serves as the main point of entry to the INDI environment for that User. As a result, this INDI Operator is also best placed to register the consent by the user as far as the release (or otherwise making available) of her personal information is concerned. This INDI Operator would then have to represent having obtained such consent towards the relevant Data Source(s). The same INDI Operator might also make a similar representation for the benefit of the Relying Party (to ensure legitimacy of the subsequent processing operations the latter plans to perform), but it is also possible that the Relying Party obtains the informed consent it needs directly from the INDI User herself in

[40] *Ibid*, 9.

[41] *Ibid*, 9.

[42] *Ibid*, 9. The controller's obligation to ensure that the data subject is properly informed about the processing is elaborated further in art. 10 and 11 of the Directive; upon which we will elaborate in section 4.9.

[43] *Ibid*, 9.

[44] Cf. *supra*; figure 1.

the context of their (application-specific) transaction. Each of these aspects will in principle need to be addressed in the contractual framework among the participants of the INDI Network.

4.4.3 Legal barriers

It is important to note that there are also instances in which consent alone may not provide an adequate legal basis for the processing. For instance, article 8a of the Directive provides Member States with the ability to specify instances in which the general prohibition to process sensitive data 'may not be lifted by the data subject's giving his consent. This provision allows national legislators to identify cases where controllers may not rely on the consent of the data subject in order to legitimize the processing. Such a provision might for example be adopted due to the particular nature of the relationship between the controller and the data subject or the risks presented by the processing.[45]

In addition, there may also be instances where sector-specific requirements prevent the disclosure of information even where the data subject has given her consent (e.g., eGovernment[46], eHealth[47]). Such requirements may prevent the disclosure of information in spite of explicit authorization by the data subject, and may prevent a barrier to the deployment of certain INDI Services (particularly in a cross-jurisdictional setting).[48] While taking note of these requirements as potential obstacles, it is also important to consider that they were adopted to protect specific interests, often those of the data subjects themselves. When assessing these obstacles from a policy perspective, one should carefully consider such interests, and whether or not an envisaged derogation might risk eroding the protection currently provided in the jurisdiction at hand.

Finally, interoperability barriers may also result from national legislation which imposes specific requirements upon consent which have not been adopted by other Member States.[49]

---

[45] The Belgian legislator made use of this opportunity by enacting art. 27 of the Royal Decree of 13 February 2001 (Koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens ['Royal Decree of 13 February 2001 in execution of the Law of 8 December 1992 relating to the protection of privacy with regards to the processing of personal data'], *B.S.* 13 March 2001) (hereafter: RD) . This article provides that the processing of sensitive data warranted solely by the consent of the data subject remains forbidden: (1) when the controller of the processing is the employer of the data subject or (2) when the data subject finds himself in a position of dependency vis-à-vis the controller. Art. 27 does list an important exception to this rule: the prohibition will not apply when the processing is designated to procure an advantage to the data subject (art. 27 in fine RD). Furthermore, for the restriction of art. 27 to apply, the processing must be based solely upon the consent of the data subject. If the controller can avail himself of one of the other legitimate bases enumerated in Belgian Data Protection Act for the processing of sensitive data, the restriction will not inhibit the processing.

[46] Cf. *infra*; section 5.2.5.

[47] In the eHealth setting medical practitioners are typically bound by a duty of professional confidentiality. In certain jurisdictions consent alone is not sufficient to relieve such practitioners of their statutory confidentiality obligations.

[48] See also See European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', November 2010, Brussels, COM(2010) 609 final, 10, available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[49] For instance, instead of requiring that the consent for processing of medical data be 'explicit', the Belgian legislator has stipulated that such consent must be given in writing (art. 7, §2, a of the Belgian Data Protection Act).

4.5 Data accuracy

Every data controller is under the obligation to ensure the accuracy of the personal data it processes (art. 6, d Directive 95/46/EC). This provision in first instance requires controllers to put in place mechanisms and procedures which enable them to establish the accuracy of data with a level of assurance proportionate to the interests at stake.[50] Art. 6, d of the Directive also stipulates that data must be kept up-to-date where necessary. This implies that controllers are in principle obliged to meet the requirement of accuracy not only at the moment of collection, but as long as the data is being processed under their control.

4.5.1 Use of authoritative sources

In the context of identity management, establishing the trustworthiness of a particular identity or attribute often involves the verification of presented data against one or more 'authoritative sources'.[51] An authoritative source can be described as a repository which is recognized as being an accurate and up-to-date source of certain information within a particular context. Such sources are typically managed by one or more entities that are functionally responsible for the collection, validation, and updating of data originating from other relevant sources (e.g., the individual concerned, a governmental agency, an organizational department, etc.).[52] Verification against authoritative sources can take place at various stages of the life-cycle of an identity and can serve different purposes (e.g., during enrolment[53], authentication[54], authorization[55], etc.). The generic purpose is typically to confirm the validity of a certain proposition (e.g., an asserted attribute, the revocation status of a credential) in real time.

[50] For example, the standard of care for ensuring data accuracy shall obviously be higher in an medical setting than in the context of social networks.

[51] See e.g. D. Chadwick, 'Federated Identity Management', in Alessandro Aldini, Gilles Barthe and Roberto Gorrieri (eds.), *Foundations of Security Analysis and Design V*, FOSAD 2007/2008/2009 Tutorial Lectures, Springer, 2009, p. 97-99.

[52] See also J.C. Buitelaar, M. Meints and B. Van Alsenoy (eds.), 'D16.1 Conceptual framework for identity management in e-government', Future of Identity in the Information Society (FIDIS) deliverable, 2008, p. 45 (available at www.fidis.net) (hereafter: 'FIDIS 16.1'). In many documents authoritative sources are also referred to as 'authentic' sources or 'authentic registers' (see e.g. the European Commission Information Society and Media Directorate-General, E-government Unit, 'A roadmap for a pan-European eIDM framework by 2010', v1.0, p. 5 (available at http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf) We have chosen to use of the term 'authoritative' as it is more in line with identity management literature and because we believe the term 'authoritative' better captures their actual role (it reflects the idea that they are seen as trustworthy within a certain context). Moreover, use of the term 'authentic' may also in the long run engender confusion with concepts such as 'authentication' or 'data authenticity' in the way traditionally used in computer sciences.

[53] For example, during the enrolment process for the issuance of a governmental eID card a Registration Authority (RA) might query the national population register to verify the accuracy of the information contained in the card that is presented by the citizen.

[54] For example, checking the validity status of a digital certificate with a Certificate Authority (be it on the basis of a Certificate Revocation List (CRL) or Online Certificate Status Protocol).

[55] For example, where an access control policy states that access to a particular resource is dependent upon a certain professional qualification.

Authoritative sources play an important role within the GINI vision. One of the key objectives of GINI is to allow users (data subjects) to link their INDI with authoritative identity data maintained by both public- and private-sector entities. These data (or links thereto) could then be presented by the user towards relying parties. The user might wish to do this in order to meet transactional requirements (e.g., access control conditions set by the Relying Party) or to improve the perception of her trustworthiness towards other INDI Users (e.g., when selling a car). The basic assumption is that Relying Parties will have greater confidence in the attributes asserted by an individual if these attributes are confirmed by an independent entity which is generally perceived as maintaining high-quality information.

4.5.2 Need for additional safeguards

Reliance upon authoritative sources is often additionally based on efficiency considerations. It allows developers to leverage existing infrastructures, and offers the advantages of having single points of contact to update and manage information.[56] This may help reduce the amount of copies of the same information in different databases, among which discrepancies may start to develop over time. Reliance upon distributed information repositories may additionally help minimize the amount of data stored centrally, which may in turn reduce the potential gain for attackers.[57] However, the actual benefits for data protection and privacy will depend largely on the implementation model and the safeguards that are put in place. Reliance upon distributed information sources implies mechanisms to make these sources 'discoverable' to authorized entities. Discovery services (sometimes also referred to as 'directory services') are services which allow authorized users to locate resources within a network, including services and entity information such as credentials, identifiers and attributes.[58] These tools do not store the actual content of the data as such, but rather provide 'pointers' to the logical location from where the information may be retrieved. However, such services may entail their own set of data protection and privacy risks, which should be considered carefully when developing an identity management framework in accordance with this model. Because discovery services and reference directories may give rise to vast data aggregation capabilities, specific safeguards must be in place to prevent abuse of their functionalities. After all, although the data no longer needs to be maintained centrally, the implementation of such tools and services in turn creates centralized data aggregation and profiling opportunities.[59] For these reasons, careful consideration should be

[56] See e.g. Deprest, J. and Robben, F., *eGovernment: the approach of the Belgian federal administration*, 2003, p. 6 available at http://www.ksz-bcss.fgov.be/binaries/documentation/fr/documentation/presse/2003_e_government_paper_v_1.0.pdf

[57] See e.g. Belgian Privacy Commission, Recommendation nr. 01/2008 of 24 September 2008 concerning user-and access management in the governmental sector, 24 September 2008, p. 4, available at http://www.privacycommission.be/nl/docs/Commission/2008/aanbeveling_01_2008.pdf.

[58] Based on International Telecommunication Union - Telecommunication Standardization Sector. Focus Group on Identity Management, 'Report on Identity Management Framework for Global Interoperability', p. 18, available at http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html.

[59] Buitelaar, J.C., Meints, M. and Kindt, E. (eds.) 'D16.3 Requirements for Identity Management in eGovernment', FIDIS Deliverable, 2009, 18, available at www.fidis.net (hereafter: 'FIDIS 16.3'). Where discovery services are both managed and operated by intermediaries, these services may additionally create centralized points from which the transactions of users may be monitored, which may in turn facilitate behavioural profiling. On the topic of profiling see also Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies, available at http://www.coe.int.

given to which entities are allowed to operate these discovery services, and which technical, organizational and legal safeguards shall be put in place to prevent abuse of their functionalities.

The designation of authoritative sources essentially involves determining which entities are trusted to act as data providers for which data items or data sets. Achieving data accuracy however in first instance implies ensuring the reliability of information before it is registered. In order to ensure that the information being maintained is in fact reliable, the designation of an authoritative source should be accompanied by appropriate policies specifying how the data will be collected, validated and kept up to date. These policies should also specify the measures that shall be used to prevent unauthorized modifications or entries.[60] Finally, appropriate measures should be adopted to ensure the authenticity and integrity of information going to and from these sources.

It is important to note that other mechanisms exist to corroborate information asserted by an individual (e.g., by relying on credentials the user has under her control without third-party verification). Which means are available and/or appropriate for ensuring data accuracy in particular context is generally application-specific.

4.5.3 Legal barriers and gaps

Despite the potential benefits, a number of legal considerations may present obstacles to the reliance upon (certain) authoritative sources. As indicated earlier, sector-specific legislation may prevent disclosure of information by the data source even where the user authorizes it (cf. *supra*). This is most notably the case for governmental agencies, where national legislation often restricts access to the information they maintain.[61] Another issue concerns the identification and communication of assurance requirements. Contrary to entity authentication (where the object of corroboration is the asserted identity of an entity), there are no commonly accepted standards for expressing assurance requirements and safeguards for attributes other than identity (e.g. professional qualifications, mandates, residency). Where a Relying Party wishes to rely upon data maintained by a third party, it will require some type of mechanism to ascertain the reliability of the data maintained by the source in question.[62] In addition, the Relying Party will also want to know to what extent it may have a legal recourse against the Data Source in cases where the information it relied upon turned out to be inaccurate. The absence of legal certainty in this regard as to the risk carried by Relying Parties and Data Sources respectively may also prove to be a barrier to interoperability.

Finally, an additional legal barrier against the re-use of information for verification purposes might also arise from the data protection requirement of finality. This issue shall be elaborated upon in the following section.

---

[60] See also FIDIS D.16.3, *o.c.*, 2009, p. 19. The articulation of such policies may also be very important from the perspective of a relying party, to allow them to assess the reliability of such information.

[61] This issue will be revisited later on in this deliverable. Cf. *infra*; section 5.2.5.

[62] In principle a relying party can 'blindly' trust the reliability of a particular attribute (e.g, because it simply believes that information maintained by the source is always accurate and up-to-date). However, where the relying party is not familiar with the issuer or its data management practices, it will require additional assurance as to the reliability of the attribute in question. This issue will be revisited later on in this deliverable. Cf. *infra*; section 4.8.3.

4.6 Finality

Article 6, b of Directive 95/46/EC dictates that personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.' This provision embodies the so-called 'principle of finality', also known as the 'purpose (or use-) limitation principle': the purpose(s) that is (are) initially specified to justify the collection and/or further processing of the data in principle delineates its authorized usage.[63]

4.6.1 Incompatible re-use

We indicated in the previous section that one of the key objectives of GINI is to enable INDI Users to present authoritative identity data about themselves to Relying Parties. The sources maintaining this information may have collected this information for any given (set of) purpose(s): customer relations management, HR management, public service delivery, member identification, etc. However, it may be expected that in many instances the context in which the user decides (or agrees[64]) to make available this information towards other entities does not match the purpose for which the data was initially collected or further processed. In other words, data which was collected for a particular purpose might be re-used for a different purpose which would arguably not satisfy the compatibility requirement set forth by art. 6, b of the Directive.[65]

4.6.2 Implications

Directive 95/46/EC allows for 're-purposing' of personal data (i.e. re-use for a purpose which cannot be considered compatible with existing purpose) only if the envisaged processing in turn meet all the requirements the law ordinarily imposes upon data processing operations.[66] This implies treating the subsequent processing operation as an entirely "new" processing operation, which must meet all the requirements set forth by the Directive.[67] In the private sector this would

---

[63] See e.g. Article 29 Data Protection Working Party, 'Working Document on the processing of personal data relating to health in electronic health records (EHR)', WP131, published online at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf, 15 February 2007, p. 6; Bygrave, L.A., 'Core principles of data protection', *Privacy Law and Policy Reporter*, vol. 7, issue 9, 2001; Kosta, E. and Dumortier, J., 'The Data Retention Directive and the principles of European Data protection legislation', *Medien und Recht International*, issue 3, 2007, p. 133. See also FIDIS 16.1, *o.c.*, 37.

[64] Although GINI aims to provide individuals with means to 'control' the disclosure of information about themselves, it may be expected that often the release of personal data will be the direct result of a request made by the collector of the information (cf. *supra*; section 4.3.2). In such contexts it might be better to refer to 'agreement' or 'assent' rather than to 'control', as the latter terminology might give rise to misconceptions as to the legal qualifications of both the collector of the information and the individual to whom the information relates.

[65] Regarding the standard to assess compatibility of subsequent processing operations see FIDIS 16.1, *o.c.*, 37-38. The Directive itself does not clearly define what constitutes a compatible purpose, which may lead to discrepancies among Member State implementations.

[66] De Bot, D., *o.c.*, p. 121 and Léonard, Th., 'La protection des données à caractère personnel et l'entreprise' ['The protection of personal data and the enterprise'], in X., *Guide juridique de l'entreprise* ['Legal guide for the enterprise'], Brussels, Kluwer, 2004, livre 112.1, p. 29. See also FIDIS D.16.1, *o.c.*, p. 37-39 and Van Alsenoy B., Kindt, E. and Dumortier, J., 'Privacy and Data Protection Aspects of e-Government Identity Management', in Van der Hof, S. and Groothuis, M.M. (eds.), *Innovating Government. Normative, Policy and Technological Dimensions of Modern Government*, Information Technology and Law Series, Volume 20, T. M. C. Asser Press, The Hague, The Netherlands, p. 255.

[67] FIDIS 16.1, *o.c.*, 38.

ordinarily require the following steps: providing (additional) notice to the data subject of this new purpose, (re-)obtaining an informed consent, additional notification to the relevant Data Protection Authority, etc. In a governmental setting this will typically entail adopting new (or expanding existing) legislation and/or obtaining authorization from national data protection authorities (where applicable).[68]

When evaluating the exchange of personal data across organizational boundaries, it is important to consider not only the purpose for which the exchange is taking place, but also to consider the role and obligations of each actor vis-à-vis this exchange. In the Personalized Identity Management (PIM) ecosystem envisaged by GINI, both the provider (Data Source) and recipient (Relying Party) of the data shall often each act as a data controller in relation to their own processing operations.[69] The storage of data by a Data Source shall in principle be the result of its own business purpose(s) (in the case of private entities) or public mission (in the case of governmental entities).[70] Similarly, the Relying Party to whom the data is made available will be collecting these data for its own purposes. Even where from a technical perspective the disclosure and collection of data might be the result of one and the same operation, they are likely to be treated as being distinct from a legal perspective (as both the Data Source and the Relying Party are likely to determine the purposes and means of their own processing operations independently of one and other, and thus in principle are separate data controllers).

To the extent that the Data Source and the Relying Party each act as a controller towards their own processing operations, they each carry the burden of ensuring compliance. As a result, the Data Source should only agree to make the information available once it has obtained sufficient assurance of either the compatibility or legitimacy (where incompatible) of the processing envisaged by the recipient. From its part, the Relying Party will similarly require a legitimate basis for its collection of personal data.

Under the GINI vision, consent is expected to act as the default basis upon which processing shall be legitimized.[71] When obtaining the consent of the INDI User, the entity collecting the consent must take care to clearly specify the purposes for which the INDI User is providing her consent. Which entity should be charged with obtaining consent for which processing operations shall depend in part on the manner in which the communication among the various actors is organized? As indicated earlier, the GINI vision assumes the presence of multiple INDI Operators who mediate trust among the different actors involved. The INDI User is not expected to communicate directly with a Data Source at the moment she wishes to obtain (a link to) verifiable data about herself, but would issue such a request towards the INDI Operator with whom she has a direct contractual relationship. This INDI Operator would then have to

[68] *Ibid*, 37-38. For instance, a prior authorization scheme was introduced in Belgium, inter alia, to help mitigate some of the risks associated with use of a single unique identifier. See http://www.privacycommission.be/en/sectoral_committees for an overview of the sectoral committees which are charged with granting or denying prior authorization for access or use of certain governmental databases and/or identifiers.

[69] See also *supra*; section 4.3.1. For the purpose of our current discussion we make abstraction of the fact that the recipient might also be another INDI User who may in certain instances benefit from the personal use exemption.

[70] We currently also make abstraction of the fact that an INDI Register might be a processor hosting the information on behalf of a controller. Where this is the case, however, the former is bound to only process the data pursuant to the instructions issued by the controller (see art. 17, 3 DPD). The legal obligation to ensure compatibility and/or legitimacy of the exchange shall be incumbent on the data controller on behalf of whom the processor is interacting, and this controller will have to authorize the processor to make available the information

[71] Cf. *supra*; section 4.4.1.

represent having obtained such consent towards the relevant Data Source(s). The same INDI Operator might also make a similar representation for the benefit of the Relying Party (to ensure legitimacy of the subsequent processing operations the latter plans to perform), but it is also possible that the Relying Party obtains the informed consent it needs directly from the INDI User herself in the context of their (application-specific) transaction.[72]

4.6.3 Legal barriers

The potential legal barriers resulting from the principle of finality are largely the same as those identified in relation to the requirements of legitimacy and the use of authoritative sources (cf. *supra*). Sector-specific legislation may prevent disclosure of information by the data source in spite of user authorization. In such instances the disclosure will only be possible where (a) the processing may reasonably be considered as compatible with the existing specified purpose (as defined within the relevant jurisdiction), or (b) a legal provision to warrant an exception to the prohibition of disclosure is adopted.

4.7 Proportionality

The principle of proportionality is a fundamental principle of data protection. Although it is not promulgated explicitly as a separate principle within the Directive, it is clearly the underlying foundation of several of the Directive's requirements, among which:

- the requirement that personal data shall be processed 'fairly' (art. 6 a);
- the requirement that personal data shall be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed' (art. 6, c); and
- the requirement that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (art. 6, e).[73]

The principle of proportionality has many different dimensions. The following subsections provide a (non-exhaustive) overview of the main implications of this principle towards personal data processing in practice.

4.7.1 Collection limitation

A first implication of the proportionality principle is that there must be a sufficiently narrow correlation, in terms of adequacy and relevancy, between the (legitimate) purpose articulated by the controller(s) and the data being collected. Only such data which are necessary to achieve the

[72] See also *supra*; section 4.4.2.

[73] For a more comprehensive overview of the role of the proportionality principle in the Data Protection Directive and EU law in generals see C. Kuner, 'Proportionality in European Data Protection Law And Its Importance for Data Processing by Companies', *Privacy & Security Law Report* 2008, vol. 07, no. 44, pp. 1615, available at http://www.hunton.com/files/tbl_s47Details/FileUpload265/2379/Kuner_Proportionality_in_EU_DataProtectionLaw.pdf.

(legitimate) aims of the controller(s) may be processed.[74] This implication of the proportionality principle is sometimes also referred to as the principle of 'data minimization'; as it requires that the least possible amount of data is processed taking into account the purpose for which it is being processed.[75]

4.7.2 Selective disclosure

Selective disclosure means that personal data should only be disclosed or otherwise made available to the extent that it is necessary to realize the purposes of the processing. This requirement acts complementary to the principle of collection limitation: the source maintaining the information should only divulge such information as needed to realize its own legitimate purposes or those of the recipient.[76]

From a practical perspective, this requirement entails inter alia that the controller is under an obligation to implement appropriate controls to limit the access/disclosure of information to those data that are needed in order to achieve the (legitimate) purposes of the processing.[77]

Moreover, where the purposes of the processing do not require the data to be made available in an identifiable form, the data should be rendered anonymous before it is disclosed.

4.7.3 Limitation of storage duration

Personal data should not be maintained longer than is necessary for the purposes for which the data were collected and/or further processed (art. 6, e). This requirement can be seen as the 'temporal component' of the proportionality principle, in that it requires deletion or anonymization of personal data as soon as it is no longer necessary.

Controllers processing information should specify in advance (i.e. prior to undertaking the processing) for how long it will be necessary to keep the information, and regularly verify that this time-frame is respected in practice.

4.7.4 Avoid unnecessary duplication

The principle of proportionality also implies that controllers should seek to minimize the number of copies of personal data being processed. The more copies are available, the greater the risk that their confidentiality or integrity might be compromised. This consideration must of course

[74] Boulanger, M.-H., De Terwangne, C., Léonard, T., Louveaux, S., Moreau, D. and Poullet, Y. 'La Protection des Données à caractère personnel en droit communautaire', *Journal de Tribunaux Droit Européen* 1997, p. 147.

[75] See e.g. Kuner, C., *European Data Protection Law – Corporate Compliance and Regulation*, second edition, Oxford University Press, New York, 2007, 73-74.

[76] Where data is made available to serve the purposes of a different controller, the entity that controls the source of the information must of course obtain prior assurance that the processing by the recipient is either (a) compatible with the purposes for which the data is currently being processed or (b) can rely on its own legitimate basis and has satisfied all the requirements the law ordinarily imposes upon data processing operations.

[77] See also *infra*; section 4.8.1.

also be balanced with the security objective of availability, which requires controllers to protect personal data against accidental destruction or loss.[78]

4.7.5 Least intrusive means

If the purposes of the processing can also be realized by less intrusive means, i.e. by means which are less likely to have an adverse impact on the privacy or other fundamental freedoms of the data subject, such means should be used.[79] For instance, if the unambiguous identification of the data subject might be ensured by other means than by using the national identification number of the individual concerned, such means should be used.[80]

4.7.6 Balance of interests

While the examples provided above have identified some of the practical implications of the proportionality principle, the 'overarching' nature of this principle also has important consequences. Because proportionality is an underlying principle of the law, it applies even if other explicit statutory requirements have been satisfied.[81] For example, even if the processing is being conducted for a legitimate purpose, and even if the data collected is both adequate and relevant in relation to that purpose, the processing may not prejudice the data subject in a way that is disproportionate in relation to the interests pursued by the controller.[82] At all times the appropriate balance between the interests of the controller and the data subject must be respected.[83]

4.7.7 Implications

The provisioning of INDI services will have to take into account each of the implications of the proportionality principle discussed in the previous subsections. Anonymous credentials provide an important building block towards achieving these objectives. Under the GINI vision, the interaction between the different INDI Operators shall be structured in such a way that it will support selective attribute disclosure and data minimization. The overall process can be summarized as follows. Initially, a user will contact a Relying Party (e.g., to request access to a service she is interested in). Having received the request, the Relying Party will respond (via its INDI Operator) with the credential-based access control policy, applicable for the resource in question. Upon receiving the policy, the INDI Operator of the User will evaluate which claims it can derive from the available credentials that fulfil the given policy, or alternatively contacts a Data Source on the fly to acquire the missing credentials. The favoured claim from the available set is then chosen by the user interactively or automatically. If the user wants to proceed, evidence for the chosen claim is generated by the INDI Operator of the User and sent, together with the claim and the attributes to be revealed, to the INDI Operator of the Relying Party. Finally, the INDI Operator of the Relying Party verifies whether the policy is satisfied by the claim and if the evidence supports the validity of the claim. If so, access to the resource is

[78] Id.
[79] Boulanger, M.-H., De Terwangne, C. a.o., *l.c.*, 147.
[80] *Ibid*, 147. See also *infra*; section 4.10.3.
[81] C. Kuner, 'Proportionality in European Data Protection Law And Its Importance for Data Processing by Companies', *l.c.*, 3.
[82] Boulanger, M.-H., De Terwangne, C. a.o., *l.c.*, p. 147.
[83] *Ibid*, 147.

granted. This approach allows users to selectively reveal a subset of their attributes or to prove that they have a credential with specific properties without revealing the credential itself or any additional information to a Relying Party.

4.8 Confidentiality and security of processing

Articles 16 and 17 of Directive 95/46/EC oblige the data controller(s) of a processing operation to implement appropriate technical and organizational measures to ensure the confidentiality and security of processing. In particular, controllers must adopt appropriate measures to 'protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access […] and against all other unlawful forms of processing.' The controller's security obligation may be qualified as an obligation of means. There are four criteria for determining the extent of this obligation, namely state-of-the-art, cost, the risks presented by the processing, and the nature of the data to be protected (art. 17, 1).[84]

Several national data protection authorities and governmental agencies have issued guidelines as to the types of organizational and technical measures data controllers should consider when handling personal data.[85] In certain jurisdictions specific security requirements have been explicitly embedded in statutory provisions.[86] In the following paragraphs we will briefly elaborate upon the main components of the controller's security obligation, and their implications for the PIM ecosystem envisaged by GINI.

4.8.1 Components

The general security obligation of controllers can be broken down into a number of components, each of which corresponds with one or more security objectives. A first security objective following from the controller's security obligation is to maintain the *confidentiality* of information. Confidentiality as a security objective can be described as keeping the content of information secret from all entities except those that are authorized to access it.[87] There are numerous approaches to providing confidentiality, ranging from physical protection to the use of access control and cryptographic algorithms.[88] In addition to safeguarding the confidentiality of information, the processing capabilities (read, write, modify …) of each entity should be limited to that which is necessary to realize the goals of the processing. This follows from a combined reading of the controller's security obligation and the proportionality principle. These

[84] Van Alsenoy B., Kindt, E. and Dumortier, J., *l.c.*, 257.

[85] These guidelines are typically adaptations of (or have been clearly inspired by) standards of the ISO/IEC 27000 Series (Information Security Management) (formerly known as ISO 17799 or BS 7799). See e.g. the guidelines issued by the Belgian Data Protection Authority: Commission for the Protection of Privacy, 'Referentiemaatregelen voor de beveiliging van elke verwerking van persoongegevens', ['Reference measures for the security of every type of personal data processing'], published online at http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf, 4 p.

[86] See Kuner, C., *European Data Protection Law – Corporate Compliance and Regulation*, second edition, Oxford University Press, New York, 2007, p. 288 et seq.

[87] Huysmans, X. and Van Alsenoy, B. (eds.), D1.3 Conceptual Framework – Annex I. Glossary of Terms, IDEM, v1.0,7 2007, p. 12 available at https://projects.ibbt.be/idem/uploads/media/2007-12-27.idem.glossary.v1.07.pdf.

[88] FIDIS D.16.3, *o.c.*, 19.

requirements apply not only at the level of each organisation, but also at the level of each individual user.[89]

Data controllers are also required to integrate appropriate security policies to safeguard the *integrity* and *authenticity* of the data.[90] Parties involved in an exchange must be able to establish whether the information emanates from an authoritative and authorized source.[91] Especially where reliance is placed upon authoritative sources, the integrity and authenticity of the data flowing to and from these sources should be protected, e.g. through use of data origin authentication protocols (which also serve to establish their integrity during transmission). Relying parties should only process personal data further if there is sufficient certainty as to its origin and integrity (i.e. upon verification that it emanates from the intended source and has not been subject to manipulation).[92]

Accountability is also often cited as an important security objective. Although the meaning of this concept varies across disciplines, as a security objective the term refers mainly to non-repudiation or general auditability requirements.[93] In this context accountability denotes that a system or protocol has been designed in such a way that relevant events can be reconstructed (e.g., in order to assess policy compliance, to determine the cause of system failure) or that plausible deniability has been diminished.[94] In other words, it refers to the need to enable traceability of the actions by entities in such a way that they might be held answerable ('called to account') if they engage in unauthorized processing activities.[95]

---

[89] *Ibid*, p. 20. See also Van Alsenoy B., Kindt, E. and Dumortier, J., *l.c.*, 258.

[90] Integrity as a security objective is understood as ensuring data has not been altered by unauthorized or unknown means (Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997, p. 32). Authenticity as a security objective is generally understood as verifiable assurance that data has emanated from the appropriate entity and has not been altered by unauthorized or unknown means (and thus the 'authenticity' of data also implies data integrity).

[91] FIDIS D.16.3, *o.c.*, p. 22.

[92] *Ibid*, p. 24..

[93] See also S. Pearson and A. Charlesworth, 'Accountability as a way forward for Privacy Protection in the Cloud', in M.G. Jaatun, G. Zhao, and C. Rong (Eds.), *Cloud Computing. First international Conference. CloudCom 2009*, December 2009, Beijing, China, 134 and P. Malone and B. Jennings, 'Distributed Accountability Model for Digital Ecosystems', *Second IEEE International Conference on Digital Ecosystems and Technologies*, 2008, 452-453.

[94] See e.g. G. Miklau, B. Levine, P. Stahlberg, 'Securing history: Privacy and accountability in database systems', *3rd Biennial Conference on Innovative Data Systems Research (CIDR)*, January 7-10, 2007, Asilomar, California, USA, 387. The concept of accountability has also received considerable attention in the policy discourse on the future regulation of data protection (see e.g. Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability', WP 173, 13 July 2010, 3, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf and European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', November 2010, Brussels, COM(2010) 609 final, 12, available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf). Our current discussion of accountability is confined to the discipline-specific meaning this concept within computer science and security literature.

[95] See also European Court of Human Rights, *I. vs. Finland*, 17 July 2008, para 41-44 (regarding the State's positive obligation to ensure implementation of adequate security measures within state hospitals to prevent unauthorized access; which may involve the maintenance of log files or other forms of 'retrospective control of data access'). Logging and auditing are generally considered standard components of information security management, and may be seen as quasi-obligatory under articles 16-17 of the Directive (see Müller, G. and Wohlgemuth, S. (eds.), 'D14.6: From Regulating Access

Data controllers are also under the obligation to protect personal data against accidental destruction or loss. This requirement can be approximated to the security objective of *availability*, which can be described as the property of being accessible and useable upon demand by an authorized entity.[96]

Finally, it is worth noting that art. 17, 1 of the Directive also contains a generic obligation to take appropriate organizational and technical measures to protect personal data against 'all other unlawful forms of processing'. This provision may be interpreted as requiring controllers to take all reasonable precautions to mitigate the risk of unauthorized processing activities by third parties or insiders.

4.8.2 Implications

As one of the main objectives of GINI is to put individuals in control of their personal information, the INDI User will have a considerable influence in determining which entities shall be considered 'authorized recipients'. However, the fact that Users are given opportunity to 'control' certain aspects of the processing doesn't absolve the other actors from their obligations under data protection law.[97] Each entity acting as a controller remains bound by the confidentiality and security obligations defined in the Directive. Similarly, each entity acting as a processor must in principle be bound to the same security obligation by means of a contract with the relevant data controller(s) (art. 17, 3). As a result, the obligation to ensure the security of processing shall in principle be the shared responsibility of the Data Sources, INDI Operators and Relying Parties that participate in a given transaction. The operational tasks related to security will have to be specified clearly in contractual arrangements among these participants. Such specifications should include inter alia:

- which entity or entities shall be responsible for authenticating the actors involved in a given transaction;
- which entity or entities shall determine the level of entity authentication assurance that is appropriate for a particular transaction, and how this shall be attained in relation to each relevant actor;
- which entity or entities shall be charged with evaluating the privileges of requesting entities and enforcing the relevant access control policies;
- which entities will be responsible for the updating of security policies in light of technical and/or legal developments;
- which entities will be charged with the maintenance of logs for which operations; and
- which entities shall be charged with regular verification of policy compliance (audit).[98]

INDI Operators are expected to assume important responsibilities in relation to the authentication of actors, as their primary role is to mediate trust across otherwise untrusted domains. It may also be expected that the INDI Operator that has a direct relationship with a particular INDI User will be charged with the registration and management of authorizations

Control on Personal Data to Transparency by Secure Logging' Future of Identity in the Information Society (FIDIS) deliverable, 2008, p. 17). It should be noted that the data contained in logs often qualifies as personal data itself (where they represent actions performed by natural persons), and are in turn subject to requirements imposed by data protection regulations (*Ibid*, p. 17).

[96] ITU-T SG 17, 'Security Compendium. Part 2 – Approved ITU-T Security Definitions', 13 May 2005, available at http://www.itu.int/ITU-T/studygroups/com17/def005.doc.

[97] See also *supra*; section 4.3.2.

[98] See also FIDIS 16.3, *o.c.*, p. 17 and Van Alsenoy B., Kindt, E. and Dumortier, J., *l.c.*, 263.

granted by this User. Data Sources and Relying Parties will in all probability remain responsible for the security of operations that take place outside of the INDI Network, but are also likely to become subject to additional obligations in light of their role within the network. The precise task allocation will depend considerably upon the implementation of the technical architecture.

4.8.3 Legal barriers and gaps

In order to adequately manage the permissions of the users of a system, one needs to put in place an identity and information security management framework. One of the first steps in the development of such a framework involves putting in place (or at least identifying) reliable identification and authentication mechanisms. To this end, more and more Member States have moved from purely paper-based identification documents towards electronic identity cards which also enable identification and authentication in a digital environment, in most cases based on Public Key Infrastructure (PKI).[99] In several instances these electronic identity cards have also been equipped with cryptographic functionalities and certificates which enable the cardholder to place qualified electronic signatures within the meaning of Directive 1999/93/EC on a Community framework for electronic signatures.[100] In addition to these authentication mechanisms, most Member States have also put in place alternative identification and authentication mechanisms (e.g., username-password combinations and/or use non-cryptographic tokens). Even in cases where notable similarities among the eID solutions adopted by Member States, each of these solutions still has its own specific properties.

One of the gaps hindering the cross-border (or cross-organizational) use of electronic identities is the absence mutual recognition. The E-Signature Directive has put in place a legal framework for the mutual recognition of qualified certificates. Once eIDs leave the 'comfort zone' of qualified certificates (where mutual recognition and liability are defined in the E-Signature Directive), trust in the eID solutions of others becomes an issue.[101] Currently there is no general assurance mechanism in place that enables this trust between countries.[102] The issue of mutual recognition was also the major obstacle identified by the eID Large Scale pilot STORK. There is currently only one Member State – Austria – that has already adopted a legal basis for the recognition of foreign eIDs.[103] Other Member States piloted based on existing recognition of qualified certificates, or limited their recognition to the pilot.[104]

---

[99] See Graux, H. and Majava, J., 'eID Interoperability for PEGS. Analysis and Assessment of similarities and differences – Impact on eID interoperability', IDABC, November 2007, p. 72 et seq, available at http://ec.europa.eu/idabc/servlets/Doc?id=29618. For transactions which only require a low level of entity authentication assurance, alternative mechanisms such as username-password combinations and other non-PKI-based tokens are also accepted. See also Hulsebosch B. a.o., 'D2.3 Quality authenticator scheme', STORK Deliverable, 2009, 44 p., available at http://www.eid-stork.eu.

[100] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *O.J.* 19 January 2000, L 13/12-20. See also *infra*; section 7.

[101] Krontiris, I., Leitold, H. Posch, R. and Rannenberg, K., 'eID Interoperability', in Fumy W. and Paeschke (eds.), M., *Handbook of eID Security – Concepts, Practical Experiences, Technologies*, Publicis, Erlangen, 2011, p. 172. As will be elaborated later on in this deliverable, the implications of the E-Signature Directive towards entity authentication mechanisms (even where they rely upon qualified certificates) is relatively limited. Cf. *infra*; section 7.9.

[102] *Ibid*, p. 172.

[103] See T. Rössler, 'Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government', *Computer Law & Security Report 2008*, vol. 24, issue 5, 451.

[104] In its Digital Agenda for Europe, the European Commission has included two key actions related to eID recognition: Key action 3 calls for a proposal of revision of the E-Signature Directive in 2011 'with

The issue of mutual recognition also arises when using credentials issued by the private sector. In both scenarios (public and private eID solutions), the setup of a common set of authentication profiles can be used in order to promote trust and interoperability.[105] In recent years, several initiatives have been undertaken in order to develop a common understanding and standardized approach to the issue of entity authentication assurance.[106] The overall approach of these initiatives is the following. They start by defining a number of assurance levels (typically four), which serve to express the degree of confidence a relying party may have that the identity claimed by a particular entity in fact belongs to that entity (e.g., 'low', 'moderate', 'high' and 'very high'). They then define the technical and organisational requirements which must be met in order to meet a certain level of assurance (LoA).[107] This approach is designed to help decision-makers to assess what type of authentication mechanisms are appropriate for which applications, and whether or not reliance on a particular eID solution is suitable for their purposes.[108] By agreeing upon a set of baseline requirements for each LoA, actors which do not have a pre-established trust relationship can make better informed decisions about whether or not to accept the credentials issued by a third party.

Trust and interoperability requires more than a common understanding about the assurance levels supported by the different eID solutions in question. For purposes of our current discussion, there are two items in particular which require additional consideration. The first item concerns the issue of oversight and enforcement of LoA requirements. The second concerns the allocation of liability in case of breach. For both items a range of different models can be envisioned. The enforcement of LoA requirements may range from complete self-assertion (no external validation or oversight) to third-party audit and certification (comprehensive validation and oversight). As far as liability allocation is concerned, one can similarly conceive of a wide range of possibilities: the relying party can rely on the eID solution 'as is' (without any ability of recourse even if the identity provider does not abide by the agreed upon practices), the identity provider might agree to indemnify relying parties to a certain amount (capped liability), an objective liability of the identity provider might be installed, there might be a pooled liability

---

a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems.' Key action 16 similarly calls upon the Commission to 'Propose a Council and Parliament Decision requesting Member States to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services''. (European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, August 2010, COM(2010) 245.) See also *infra*; section 7.9.

[105] Krontiris, I., Leitold, H. Posch, R. and Rannenberg, K., 'eID Interoperability', *l.c.*, p. 172.

[106] See e.g. W.E. Burr, D. F. Dodson and W.T. Polk, Electronic Authentication Guideline, NIST SP800-63, v1.0.2, available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf; Graux, H., Majava, J., 'eID Interoperability for PEGS - Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms', IDABC, December 2007, available at http://ec.europa.eu/idabc/en/document/6484.html; Glade, B., 'Identity assurance framework: Assurance Levels', v2.0, 24 April 2010, Kantara Initiative, available at http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework+v2.0. ISO/IEC JTC 1 SC 27/WG 5 and the ITU-T are currently also developing a joint standard in relation to entity authentication assurance (29115/X.eea).

[107] These requirements are typically compartmentalized according to different phases of the authentication process (e.g. registration of users, credential issuance, strength of authentication mechanism, safeguards implemented during credential usage etc.).

[108] Determining the requisite LoA for a particular application is done by performing a risk analysis, which similarly leads a risk classification (e.g., low, moderate, high etc.) which can then be mapped to the LoA scheme.

scheme jointly funded by the participants in a federation, etc. The configuration of these parameters (enforcement, oversight, liability exposure, recourse) will influence both the trust decision of relying parties, as well as the willingness of identity providers to make their services available to third parties. Absence of (legal) certainty in this regard may pose a considerable barrier to interoperability and the development of mutual trust relationships.[109]

Similar considerations apply in relation to the certification of (and reliance upon) attributes other than identity. Here the question is not whether or not the identity claimed by a particular entity in fact belongs to that entity, but rather whether or not the entity in question in fact has the attribute that is being asserted/required in the context of a particular transaction (e.g., a professional qualification, a legal mandate, a role). Although theoretically a similar approach as the one adopted in relation to the issue of entity authentication assurance is possible (the digital identity of entity is in fact also just an attribute of that entity), this area is far less developed.

A final issue which merits further elaboration relates to the integration of national identification numbers in eID solutions (e.g., the inclusion of a national identification number in the public-key certificate contained in an eID card). Several Member States have opted to regulate the use of such identification numbers; restricting the type of entities that are allowed to use them.[110] Where these numbers have been integrated in a particular eID solution, these regulations can pose a de facto barrier to the reliance upon these credentials across (jurisdictional or organizational) boundaries. This issue shall be revisited later on in this deliverable.[111]

4.9 Transparency and data subject rights

Articles 10 et seq. of Directive 95/46/EC set forth the transparency obligations of data controllers and list the rights data subjects can exercise towards controllers when their personal data is being processed. Underlying these provisions is the idea that the data subject should in principle:

- be notified of the processing of her personal data (notice);
- have means to obtain further information (right of access); and
- have immediate means of recourse towards the controller in case she feels her data are being processed improperly (right to rectification, erasure or blocking).

Each of these rights shall be elaborated further in the following subsections.

4.9.1 Notice obligation

Articles 10 and 11 of the Directive specify which information controllers must provide data subjects in relation to the processing of their personal data. These provisions aim to render the data processing transparent towards the individuals concerned. Such transparency is a necessary precursor for the data subject to be able to exercise her rights as a data subject: if the subject is not aware of the processing, she will not be able to scrutinize the processing and make a

[109] In case of 'closed' systems (i.e. systems which are based on voluntary agreements between a specified number of participants) the requisite legal certainty can be established through contractual means. See also *infra*; section 7.12.

[110] Cf. *infra*; section 4.10.2.

[111] Id.

determination as to whether or not to object to the processing, or whether she wishes to submit a request to see her data amended, etc.

When reviewing the controller's notice obligations, a distinction can be made between two scenarios: one in which the information is obtained directly from the data subject (art. 10), and one in which the information is collected indirectly (i.e. from an entity other than the data subject) (art. 11). The notice obligations in each scenario are relatively similar; the main relevance of the distinction concerns (a) the moment by which notice must be provided[112] and (b) the exemptions to the notice provision.[113]

As a rule, each data subject must at least be informed of the identity of the controller (and, if applicable, of his representative) and the purposes of the processing. Additional information may be required in instances where this can be deemed necessary in order to guarantee fair processing in respect of the data subject. Such further information might include:

- the categories of data concerned;
- the recipients or categories of recipients; and
- the existence of the right of access to and the right to rectify inaccurate data.

The controller's obligation to provide notice of the elements mentioned above is based on a number of premises, among them the notions:

- that individuals need to be able to make 'informed' decisions when contemplating whether or not to authorize the usage of their personal data (cf. the requirement that the consent given by the data subject be 'informed'); and
- that of accountability: such notices are expected to provide reference documentation which should (in principle) allow both individuals and enforcement authorities to assess compliance on a post fact basis (cf. the requirement of specificity in both the purpose specification principle and the definition of data subject consent).

Controllers typically acquit themselves of their notice obligations by posting a privacy policy on their website, or by incorporating the requisite information elements in the consent form presented to the data subject. Despite the potential benefits of privacy notices, the efficacy of the current notice obligations is more and more being called into question. Three vulnerabilities in particular are often cited:

- the general risk of 'information overkill', as a result of which individuals no longer read, or merely gloss over notices of privacy practices;
- overly 'legalistic' drafting of such notices: as a document with potential legal implications, such notices are often drafted in a way that they are difficult to understand for non-legal experts; and
- the technical complexity of (and in certain instances, the controller's wish to obfuscate) data processing operations, together with the continuous change in actors and processes,

[112] In case of direct collection notice must in principle be provided at the moment of collection (or earlier) (art. 10). In case of indirect collection, notice must in principle be provided 'at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed' (art. 11, 1).

[113] In case of indirect collection, art. 12 provides exemptions to the notice obligation where the processing is being carried out 'for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law.' Member States are however expected to provide for appropriate safeguards for such instances in their national legislation.

push drafters of such notices towards abstraction (which in turn renders them relatively meaningless).

In 2004, the Article 29 Working Party adopted an Opinion on the development of standardized notices and more harmonized information provisions.[114] This Opinion outlined a 'layered approach'[115] towards fulfilling notice obligations to help mitigate risk of complexity.

In its Communication outlining potential means for strengthening the current data protection framework, the European Commission has reaffirmed the fundamental importance of transparency of data processing. It is considering the introduction of a general principle of transparent processing of personal data in the current legal framework. In the same Communication the Commission also echoed the Working Party's call for further development of standardized information notices. [116]

4.9.2 Right of access

Art. 12 stipulates that every data subject shall have the right to obtain from the controller, without constraint, at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to her are being processed;
- information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
- communication to her in an intelligible form of the data undergoing processing and of any available information as to their source; and
- knowledge of the logic involved in any automatic processing of data concerning her at least in the case of the automated decisions.

The precise modalities of how data subjects can exercise these rights are specified in national legislation. Controllers often maintain a considerable margin of appreciation as to how they accommodate the data subject requests for access. Data subjects typically do not have the right to exact that the controller provides the relevant information in a particular format or carrier.

An interesting question is whether the data subject right of access may be delegated by the data subject to another party. The Directive itself does not provide any indication either way on this issue. In certain jurisdictions the legislation implementing the Directive explicitly states that a right of access request might be exercised by a 'legal representative' (e.g., the legal guardian of a minor). The extent to which individuals are free to contractually delegate their right of access to third parties (e.g. a service provider) is less clear. In principle there is no restriction towards doing so, provided that the requirements for the validity of delegation contracts in general are met.[117] This includes the general requirements that the object and cause of the contract must be lawful, and may not serve as a legal construct aiming to circumvent statutory restrictions.[118]

---

[114] Article 29 Data Protection Working Party, 'Opinion on More Harmonised Information Provisions', WP100, 25 November 2004.

[115] Under such an approach not all information is provided in a single document, but rather spread out of over a number of layers of information (short – condensed – full).

[116] See European Commission, 'A comprehensive approach on personal data protection in the European Union', *l.c.*, 6.

[117] See also De Bot, D., *o.c.*, 223.

[118] For instance, one might argue that a construct whereby a service provider relies upon a delegated access right in order to gain access to information for which it otherwise would require a specific statutory provision or prior authorization would be invalid.

Even where the delegation of the right of access might be considered lawful, the national requirements concerning the form in which the data subject must exercise her right of access must also be taken into account.

4.9.3 Right to rectification, erasure or blocking

Article 12, b of the Directive stipulates that data subjects have the right to obtain, as appropriate, the 'rectification, erasure or blocking' of data in case where the processing of which does not comply with the provisions of the Directive. Rectification shall be particularly appropriate in instances where the data being processed is found to be inaccurate. However, this provision also enables data subjects to request the deletion or blocking of data where it appears the data has been obtained unlawfully or there is no longer a legitimate need to maintain the data.

In instances where the data subject's request for amendment, deletion or blocking is granted, she may also request that controller provides notification thereof to any third parties to whom the data have been disclosed. The only grounds for the controller to refuse such a request would be to assert that such notification is impossible or involves a disproportionate effort (art. 12, c).

4.9.4 Implications

Ensuring adequate transparency and availability of effective mechanisms for exercise of data subject rights can be challenging in complex processing environments. Each entity acting as a controller is in principle required to provide notice for those processing operations it controls, and to accommodate data subject requests concerning access, rectification, erasure or blocking. However, if each entity acting as a controller were to try to acquit itself from these obligations independently of one and other, this would have a number of unwanted consequences. In first instance, every INDI User might receive up to five different notices[119] for what it perceives as one and the same functionality. It might become very unclear whom she should address in case of a complaint, or to whom she should direct her requests for information, corrections or access to personal data.[120] Secondly, not every actor will necessarily be in direct communication with the data subject at the moment that the processing is being authorized. Sending separate ('out-of-band') notices would not only give rise to additional confusion, but might also imply considerable administrative overhead.

For these reasons a more integrated approach is necessary, which considers the overall functionality that the INDI Network aims to provide its end-users. As far as the notice obligation is concerned, a possible approach would be that the INDI Operator (who has a direct relationship with the INDI User to whom the information relates) would initially provide its Users with a 'comprehensive' notice. This notice would cover not only its own processing operations but also provide a general notice with regard to the information exchanges between the other actors participating in the INDI Network. Each actor would then still post a privacy notice on its own webpage, which would provide further details of its specific operations. This notice might also cross-reference the notice provided by the INDI Operator. In any event, at the moment of authorization, the INDI user should be given an integrated notice relating to the

[119] Cf. *supra*; section 4.3.1.

[120] See also Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', *l.c.*, 24. The Working Party has indicated that such a situation would risk making the entire processing unlawful due to a lack of transparency and violate the principle of fair processing (*Ibid*, 24).

transaction at hand. [121] This could be done in a condensed format, providing links to more detailed notices, allowing the INDI User to 'drill down' and obtain more information about the various aspects of the processing.

As far as the data subject rights of access, rectification, erasure or blocking are concerned, a complementary approach could be adopted. The general notice provided by the INDI Operator should specify:

- to whom data subjects should address their access request, objection, or request for rectification in relation to data processed in the context of INDI transactions;
- which actor(s) will be competent to decide about those requests;
- a procedure in case the data subject submits a request to an actor which is not competent in deciding about those requests.[122]

Of course, the participants in the INDI Network will have to establish which actor will be competent to decide which requests, as well as what consequences shall be triggered where a request is granted (e.g., notification of other entities to whom the data has been disclosed where appropriate to ensure they make the necessary modifications). The participants should also agree among each other on the procedures that will be followed in case the data subject submits a request to an actor which is not competent in deciding about those requests.[123]

4.10 Identifiers of general application

Article 8.7 of Directive 95/46/EC provides that 'Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.' Every Member State has since defined its own national policies concerning the use of such identifiers, among which there exist substantial differences. Several studies since then have been carried out to compare the various approaches, and to identify the barriers they present in the context of pan-European eGovernment services.[124] In the following sections we will identify

[121] This approach was inspired by the recommendations issued by the European Data Protection Supervisor (EDPS) in the context of the development of the Internal Market Information (IMI) system. See European Data Protection Supervisor, 'Opinion on the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC)', O.J. 25.10.2008, C 270/1-7, considerations 36-38.

[122] See also EDPS, 'Opinion on the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC)', *l.c.*, consideration 37.

[123] In the context of the IMI system, Recommendation 2009/329 provides that: 'no competent authority should refuse access, rectification or deletion on the ground that it did not introduce the data in the system or that the data subject should contact another competent authority. The competent authority receiving the request will examine it and grant or refuse it in accordance with the merits of the request and the provisions of its own national data protection law. If necessary and appropriate, the competent authority may contact other competent authorities before taking a decision.' (European Commission, 'Commission Recommendation 2009/329/EC of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI)", O.J. 18.04.2009, L 100/12-28, pp. 25-26.)

[124] See e.g. Dos Santos, C. and De Terwangne, C., 'Privacy and Data Protection in eGovernment' in X., 'Breaking Barriers to eGovernment - Overcoming obstacles to improving European public services', Modinis study, 2006, p. 133-136, available at www.egovbarriers.org; H. Graux, J. Majava, E. Meyvis (eds.), 'Study on eID Interoperability for PEGS: Update of Country Profiles - Analysis & assessment report', October 2009, IDABC, p. 122-128, available at

the main issues concerning the use of identifiers of general application and their implications for the deployment of INDI services.

4.10.1 Use of unique identifiers

Unique identifiers are generally considered to be an inevitable part of any identity management system. In first instance they are deemed necessary in order to ensure unambiguous identification of both the resources and the users of a particular information system. Unique identifiers help ensure that information is linked to the appropriate account, enable easy (re)identification of returning users, and facilitate the exchange of information about a particular entity. Without unique identification there is also a risk that entities displaying similar attributes (e.g., first and last name) are mistaken for one and other and that as a result the wrong information is retrieved or that information is associated with the wrong entity. In other words, unique identifiers can help ensure the accuracy of the data being processed by enabling the system to efficiently 'single out' the entity about (or from) which one wishes to retrieve or exchange information.

Unique identifiers relating to individual persons are often referred to as 'personal identification numbers'.[125] The increased use of personal identification numbers has triggered a number of concerns within privacy and data protection communities. The major concerns relating to personal identification numbers do not relate to the usage of unique identifiers as such, but rather to the consistent use of the same identifier across a multitude of contexts and/or sectors.[126] The central notion underlying these concerns is that where individuals are consistently identifiable in the same manner, this may create (or at least facilitate) opportunities for unlawful data exchange, data aggregation and profiling.[127]

4.10.2 National regulation and protection of identifiers of general application

In light of the concerns articulated in the previous section, several Member States have opted to regulate the use of personal identification numbers, in particular those that are issued and used by governments. As already indicated, there exist substantial differences among these national identifier policies. The IDABC Study on Interoperability for PEGS[128] has provided an overview

http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521; and Leenes, R., Priem, B., Van de Wiel, C. and Owczynik, K., 'D2.2 Report on legal interoperability', STORK project, 2009, p. 40-41, available at https://www.eid-stork.eu.

[125] See Council of Europe Committee of experts on data protection (CJ-PD), 'The introduction and use of personal identification numbers: the data protection issues', study prepared under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1991, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports_and_studies_en.asp.

[126] See also Buitelaar, J.C. (ed.), 'D13.3 Study on ID number policies', FIDIS Deliverable, 2007, p. 23, available at www.fidis.net.

[127] For a more detailed overview of the of the privacy risks that may emerge in case of systematic or extended recourse to the same identifier across contexts and sectors (in particular when identifiers are propagated and used beyond the domain of applicability for which they were originally intended), see Van Alsenoy, B. and De Cock, D., 'Due Processing of personal data in eGovernment? A case study of the Belgian electronic identity card', *Datenschutz und Datensicherheit*, March 2008, pp. 180-181, available at http://www.fidis.net/fileadmin/fidis/publications/2008/DuD-2008-03-Due-processing-of-personal-data-in-eGovernment.pdf. See also FIDIS D16.1, *o.c.*, pp. 43-46.

[128] See http://ec.europa.eu/idabc/en/document/6484.html.

of the various policies of Member States regarding the use of identifiers of general application and grouped them into three main categories[129]:

- 'Unprotected': unprotected identifiers are not subject to any specific restrictions regarding their use and are completely open for private sector uptake;
- 'Restricted': restricted identifiers may only be used within a specific context (e.g. social security or tax administration);
- 'Protected': protected identifiers may only be used after obtaining specific permissions, either directly by law, or through a specific public sector body (e.g., national data protection authority).

The majority of Member States currently do not allow national identification numbers to be used outside the Member State itself. [130] In Belgium, use of the national registry number is restricted to legally authorized entities, and often requires (additional) authorization by (a dedicated Sectoral Committee of) the Data Protection Authority.[131] Certain Member States even constitutionally oppose the use of identifiers of general application altogether (e.g. Germany, Hungary). Other Member States have more permissive policies, allowing for unrestricted use within both public and private sectors (e.g., Sweden).[132]

In addition to regulatory solutions, several Member States have also introduced additional technical and organizational safeguards to help prevent the unlawful use of personal identification numbers. For instance, in Austria, a sector-specific identification approach is followed, which can be outlined as follows. During the issuance process, the person's Citizen Card[133] is initialized with a sourcePIN (sPIN). This sourcePIN is created by the Source PIN Register Authority (which is under the control of the Austrian Data Protection Authority) on the basis of the 'base register number' of a private person.[134] The sourcePIN may only be stored in the person's Citizen Card.[135] This sourcePIN can be used to calculate sector-specific personal identification numbers (ssPINs) that serve to uniquely identify a citizen within a specific sector.[136] When using the Citizen Card in an authentication process, the sourcePIN is cryptographically transformed to derive an sector-specific PIN (ssPIN). This enables unique identification of the

---

[129] H. Graux, J. Majava, E. Meyvis (eds.), 'Study on eID Interoperability for PEGS: Update of Country Profiles - Analysis & assessment report', October 2009, IDABC, 115, available at http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521.

[130] See Leenes, R. a.o., 'D2.2 Report on Legal Interoperability', STORK Deliverable, 2009, 163 p., available at http://www.eid-stork.eu., in particular p. 32 and 40.

[131] See Van Alsenoy, B. and De Cock, D., 'Due Processing of personal data in eGovernment? A case study of the Belgian electronic identity card', *l.c.*, p. 181.

[132] See Van de Zande, N., 'Identification numbers as pseudonyms in the EU public sector', forthcoming.

[133] The Austrian Citizen Card is not merely a certain type of card but rather a concept defined by a set of technical specifications. The implementation of this concept can be realized by means of a smart card, but can also be realized using any other technical device which fulfils the requirements specified in the concept (T. Rössler, *l.c.*, 450-451.).

[134] The base register numbers of a private person are maintained either in the Central Residents Register or Supplementary Register. These numbers are not used as unique identification numbers in the Austrian electronic identification system. The usage of these numbers is restricted by law to certain well-defined purposes. (T. Rössler, *l.c.*, 448.)

[135] *Ibid*, 449. As a result, there is in fact no central register storing all sourcePINs (despite the fact that the entity creating the sourcePIN is called 'Source PIN Register Authority). However, the Source SPIN Register is allowed to recreate a citizen's SPIN without involving the citizen or her Citizen Card in certain legally defined circumstances. (Id.).

[136] De Cock, D., 'Contributions to the Analysis and Design of Large-Scale Identity Management Systems', Dissertation present in partial fulfillment of the requirements for the degree of Doctor in Engineering, K.U.Leuven, June 2011, p. 17. See also T. Rössler, *l.c.*, 448-449.

person within a government sector (health, tax, etc.) or within one company, but cross-correlating these identifiers across sectors of companies is technically inhibited, unless the citizen herself or – in legitimate cases – the Data Protection Authority establishes such a cross-sector link.

The German eID card also supports the creation of sector-specific identifiers. In addition, access to the information contained on the card (first and last name, DOB, etc.) is restricted to authorized entities. Only service providers which have been explicitly approved by the Department for Authorization Certificates (VfB) may read data from the identity card.[137] A permission to read data from the identity card requires approval by the VfB.[138] This requirement applies in addition to the basic requirement that the card holder must grant permission by entering her secret PIN-number.[139]

4.10.3 Implications

Even where they are not subject to specific regulation, personal identification numbers still qualify as personal data and therefore remain subject to the general data protection requirements set forth by the Directive. As a result, the choice for the use of a certain identification number must satisfy the requirements of adequacy, relevancy and proportionality.[140] Use of an identifier of general application can be excessive in relation to the purposes of a particular processing operation. For instance, if at the moment of a data exchange there is no legitimate reason for the recipient of data to use the identification number, this number should not be exposed to the recipient.[141]

Use of existing identifiers is in principle also bound by the principle of finality, which implies that they should not be further processed in a manner that is incompatible with the purpose for which they were initially collected (created).[142]

Finally, consideration should also be given the controller's obligation to ensure the confidentiality and security of processing. This obligation entails that controllers must adopt appropriate measures to 'protect personal data […] against all other unlawful forms of processing'.[143] Given the finding that extended recourse to the same identifier may facilitate unlawful data exchange, data aggregation and profiling, the dissemination of identification numbers should be minimized.

The national regulations on the use of identifiers of general application, together with the restrictions following from the general data protection requirements, entail that the identification numbers used at the level of the Data Source should in principle not be disclosed to Relying Parties. This may, at least from a technical perspective, create additional challenges for the development of INDI Services.

---

137 See Fromm, J. and Hoepner, P., 'The New German eID card', in Fumy W. and Paeschke (eds.), M., *Handbook of eID Security – Concepts, Practical Experiences, Technologies*, Publicis, Erlangen, 2011, 155-157. See also Hornung, G. and Roβnagel, "An ID card for the Internet – The new German ID card with 'electronic proof of identity", Computer Law & Security Review 2010, vol. 26, p. 154 et seq..

138 Fromm, J. and Hoepner, P., 'The New German eID card', *l.c.*, 157.

139 *Ibid*, 157.

140 Cf. *supra*; section 4.7.

141 See also FIDIS 13.3, *o.c.*, 31.

142 Cf. *supra*; section 4.6.

143 Cf. *supra*; section 4.8.

In all probability, and identifier conversion mechanism of some form will be needed in order to respect the 'boundaries' of the domain of application of each personal identification number (whether this domain be national, sectoral, or at the level of every relying party).

In STORK, a principle of territoriality was followed, which was based on the rules of the jurisdiction in which a service provider receiving an identifier is followed. If a Member State has a legal basis for using the same unique identifier across sectors within its jurisdiction, an identifier received from another country may as well be used the same way. The Member State sending the identifier may however derive specific identifiers in order to comply with its own measures. Vice versa, if a Member State defines particular protection for identifiers, an identifier received from another Member State deserves the same level of protection. In addition, STORK defined cryptographic protocols that might be used to derive identifiers on a state, service provider, or application granularity. This technical measure is an option a Member State may choose on top of the territorial principle defined before.

5 Re-use of public sector information

5.1 Governmental departments as authoritative sources

One of the key objectives of GINI is to allow users of INDI Services to link their INDI with authoritative identity data maintained by both public- and private-sector entities.[144] Governments maintain a vast amount of information about their citizens. A considerable portion of this information might at some point be relevant in the context of INDI Services. Relevant data might for instance be included in population, company, vehicle or credit registers or registers maintained by employment agencies. While the quality of this information may vary in practice, it is often presumed to be trustworthy.[145] Leveraging these data could therefore in principle enhance the credibility and trustworthiness of the digital identities used within the personal IDM ecosystem.

Re-use of public sector information is the topic of Directive 2003/98/EC, the so-called PSI Directive. Over the following subsections we will elaborate the objectives of this Directive, whether it applies to the provisioning of INDI Services, its substantive provisions, and the extent to which this Directives creates any enablers or barriers towards the provisioning of INDI services that seek to rely on data maintained by governmental departments.

5.2 Directive 2003/98/EC[146]

In 2003, the Council of Ministers and the European Parliament adopted Directive 2003/98/EC on the re-use of public sector information.[147] The main purpose of this Directive is to harmonise the policies and practices of the Member States with regard to the re-use of data held by public sector bodies. While the importance of PSI for the entire society was recognized, the main target group of the PSI Directive was the information industry creating information products and services based on bulk data from the public sector.

The PSI-Directive was the result of a long process towards the establishment of a European information market, started by the European Commission in the 1980s. It established a minimum

[144] See also *supra*; section 4.5.1.

[145] The actual degree of trustworthiness will of course vary per attribute, and depend on the level of assurance provided by procedures surrounding the registration, validation and maintenance of these attributes. Nevertheless, many European governments assume the role of primary identity provider (through the issuance of ID cards, be they electronic or paper-based) and act as the 'official' source for many basic attributes such as date of birth, current address, marital status, current occupation etc.

[146] This subsection is comprised primarily of extracts of the following two publications: Janssen, K., "The PSI directive – running behind before it even started?" in E. Schweighofer, J. Gaster and B. Farrand (ed.), *Knowright 2010 Proceedings. Knowledge Rights – Legal, Societal and Related Technological Aspects*, 129-139 and Janssen, K., "The role of public sector information in the European market for online content services: a never-ending story or a new beginning?", in X., *Online content: poly and regulation for a global market - EuroCPR 2011*, March 2011.

[147] *European Parliament and Council,* Directive 2003/98/EC on the re-use of public sector information, OJ L 345, pp. 90-96 (2003).

set of rules governing the re-use and the practical means of facilitating the re-use of existing documents held by public sector bodies of the Member States. The Directive had to be transposed by 1 July 2005. Only four Member States made this deadline. By May 2008, all Member States had notified complete transposition of the Directive.[148]

5.2.1 Scope

The PSI-Directive applies to the re-use (and facilitation of re-use) of existing documents held by public sector bodies of the Member States (art. 1).

A document is defined as "(a) any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording; (b) any part of such content" (article 2.3). "Re-use" is defined as the use of public sector documents "for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced. Exchange of documents between public sector bodies purely in pursuit of their public tasks does not constitute re-use" (article 2.4 of the PSI directive). Hence, re-use comprises any use of documents held by public sector bodies, whether for commercial or non-commercial purposes, except for two types of use: use for the initial purpose within the public task for which the document was created, and the exchange of documents between public bodies purely for public task purposes. The definition of re-use is very broad in the sense that it includes all commercial and non-commercial use and not just the creation of information products and services by the information industry, as was originally intended by the European Commission.

Several types of documents are excluded from the field of application of the PSI-Directive.[149] First, the PSI Directive exempts documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned. Value-added products that are sold on the market in competition with the private sector do not have to be made available for re-use under the conditions of the Directive.[150] Second, documents for which third parties hold the intellectual property rights are exempted, as only these third parties can give permission for the further use of the documents, and not the public bodies. Third, documents excluded from access by virtue of the access regimes in the Member States (e.g. on the grounds of the protection of national security, or statistical or commercial confidentiality) are not re-usable.[151] Fourth, documents from particular institutions are not subject to the re-use regime of the PSI Directive: documents held by public service broadcasters, by educational and research establishments, and

[148] In the meantime, Belgium, Spain, Luxembourg and Austria had been convicted by the European Court of Justice for not transposing the directive in time. In the course of 2009, the European Commission has also taken action against Sweden, Poland and Italy for failing to fully or correctly implement the directive (see *Commission of the European Communities website,* Public Sector Information, http://ec.europa.eu/information_society/policy/psi/index_en.htm.

[149] See article 1 of the PSI directive.

[150] This exemption envisages the situation where the documents maintained by public sector body were developed independently of the public task. However, a public sector body is also re-using its own documents if it creates an information service or information product that should be considered a commercial product offered on the market rather than a part of the execution of the public task. This entails that any information that is used by this public body as a resource for an information product or service, also has to be available to its competitors from the private sector.

[151] This is only logical: documents that cannot be accessed for the protection of other public or private interests can also not be re-used.

by cultural establishments.[152] While these institutions hold a lot of information that would be very valuable for the private sector to re-use, these exemptions were included in the Directive because of the particular situation of these organisations, which in many cases have to ensure part of their budget from the valorisation of their information (e.g. universities patenting their research, museums selling art books and posters).[153]

The scope of the PSI Directive does not a priori exclude identity attributes related to citizens as being public sector information. This Directive could therefore in principle be relevant to the development of INDI services where the aim is to allow users to link their INDI with authoritative identity data maintained by a public sector entity. The substantive provisions of the Directive will be elaborated in the following sections.

5.2.2 Basic principles

The first basic principle of the PSI Directive is the *absence of a general obligation to make public sector documents available for re-use*. While the PSI directive encourages re-use, it does not impose any obligation on the Member States to make their documents available for re-use as such. Only if they (or their public bodies) choose to do so, they will have to comply with the obligations of the Directive and the transposing national legislation.

The second basic principle of the PSI-Directive is the principle of *non-discrimination*. Once certain public sector information has been made available for re-use within the meaning of the Directive, the public sector body must in principle make this information available for re-use by other entities in a non-discriminatory fashion. Specifically, article 10 provides that 'any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use'. Complementary to the principle of non-discrimination, the PSI Directive provides for a *prohibition of exclusive arrangements*. The re-use of public sector documents must be open to all potential actors in the market, even where one or more market players already exploit added-value products based on these documents. Consequently, contracts or other arrangements between the public sector bodies holding the documents and third parties may not grant exclusive rights (art. 11, 1). The only exception recognized by the Directive in this regard is where the granting of an exclusive right is necessary for the provision of a service in the public interest (art. 11, 2).[154]

The third basic principle set forth by the PSI-Directive is the principle of *transparency*. Several provisions of the PSI Directive are aimed at ensuring transparency towards potential re-users of PSI. In first instance these provisions concern the communication of opportunities for (and conditions related to the) re-use of PSI (art. 9). The PSI Directive also requires public sector bodies to communicate grounds for refusal as well as possible means for redress (art. 4). These transparency obligations are intended to support the overall objective of the PSI objective, which is to ensure 'level playing field' which enables real and effective competition.

---

[152] For cultural establishments, comparable questions are currently being dealt with in the Europeana initiative.

[153] Janssen, K. and Kabel, J.J.C., "Commercialisering van overheidsinformatie door de overheid: rechtspraak en wetgeving in België en Nederland", *Computerrecht* 2005, no. 3, 126; Pas, J. and De Vuyst, B., "Re-Establishing the Balance between the Public and the Private Sector: Regulating Public Sector Information Commercialization in Europe", *Journal of Information, Law and Technology* 2004, no. 2, 11.

[154] The validity of the reason for granting such an exclusive right shall be subject to regular review, and shall, in any event, be reviewed every three years. The exclusive arrangements established after the entry into force of this Directive shall be transparent and made public (art. 11, 2).

In addition to three basic principles, the PSI-Directive also outlines a number of requirements in relation to the processing of requests of re-use, as well as for the conditions and licenses which might be imposed upon re-use. These requirements will be elaborated briefly over the following two subsections.

5.2.3 Requirements for the processing of requests of re-use

Article 4 outlines a number of requirements for the processing, by public sector bodies, for the processing of requests of re-use. These requirements concern the time limits, communication of the grounds for refusal, and references to the possible means of redress.

According to article 4.1 of the PSI Directive, public sector bodies "shall, through electronic means where possible and appropriate, process requests for re-use and shall make the document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the timeframes laid down for the processing of requests for access to documents." This provision entails that, where a Member State has adopted freedom of information (FOI) legislation, it should in first instance have regard to the time frames specified there to determine the appropriate time limits.[155] Where no time limits or other rules regulating the timely provision of documents exist, public sector bodies must in principle process the request and deliver the documents not more than 20 working days after its receipt.[156] This timeframe may be extended by another 20 working days for extensive or complex requests. In such cases the applicant shall be notified within three weeks after the initial request that more time is needed to process it (art. 4.2).

In the event of a negative decision, the public sector bodies must communicate 'the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or of the national provisions adopted pursuant to this Directive' (art. 4.3). Any negative decision also has to contain a reference to the means of redress in case an applicant wishes to appeal that decision (art. 4, 4).

The obligation to state the grounds for refusal and to specify possible means of redress is one of the big merits of the Directive. Before the Directive, public sector bodies could in principle refuse the request for re-use without letting the applicant in on the reason, or without specifying whether and how the decision might be appealed.

5.2.4 Conditions for re-use

Where public sector information is made available for re-use, a number of conditions must be met. These conditions relate to the format of the documents, charging, transparency, licensing, and practical arrangements for facilitating the search for documents.

Pursuant to article 5.1, public sector bodies must make their documents available 'in any pre-existing format or language, through electronic means where possible and appropriate'. Public sector bodies are by no means obligated to create or adapt documents pursuant to a request. Art.

[155] Idem

[156] In case a license is needed, the first license offer should also be finalized within that same timeframe (art. 4.2).

5.1 also specifies that public sector bodies are not obliged to provide extracts from documents where this would involve disproportionate effort.

As far as charging is concerned, the PSI Directive specifies that the total income from supplying and allowing re-use of documents shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment (art.6).[157] In doing so, the PSI Directive leaves a considerable margin of appreciation to the Member States and public sector bodies, 'having due regard to the self-financing requirements of the public sector concerned, where applicable'.[158] It only imposes an upper limit to the charges (reasonable return on investment), but no criteria on how to determine whether the charged amount is reasonable or not.

Public sector bodies are allowed to impose certain conditions upon the re-use of public sector information. Such conditions may be imposed by means of a license, but they may also be imposed through other means (art. 8). Article 8 does not regulate the terms of licenses in great detail. It merely states that if licenses are used they 'shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition' (art. 8.1). The Directive does require Member States to encourage the use of standard licenses, but it does not demand a particular result (other than the fact that such licenses are available in a digital format and can be processed electronically).[159]

Finally, art. 9 specifies that 'Member States shall ensure that practical arrangements are in place that facilitate the search for documents available for re-use, such as assets lists, accessible preferably online, of main documents, and portal sites that are linked to decentralised assets lists'. The main objective of this provision is to ensure that potential re-users of information have the means to learn of the opportunities for doing so.

5.2.5 Relationship to Directive 95/46/EC

A considerable portion of the information held by public sector bodies can be considered as personal data within the meaning of Directive 95/46/EC. The PSI directive does not exclude such data from being re-used, but it states explicitly that it 'in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Community and national law, and in particular does not alter the obligations and rights set out in Directive 95/46/EC' (art. 1, 4). In other words, the PSI Directive does not affect the harmonized level of data protection rules as set out in Directive 95/46/EC.[160] Any request for re-use of public sector documents containing personal data will consequently still need to be evaluated against the requirements of the Data Protection Directive.

We have already elaborated upon the substantive provisions of Directive 95/46/EC in the previous chapter. However, there are three principles which merit further elaboration for the purposes of our current discussion, namely the principles of legitimacy, finality and lawfulness.

---

[157] Charges should also be cost-oriented over the appropriate accounting period and calculated in line with the accounting principles applicable to the public sector bodies involved (art. 6).

[158] Recital (14) of the PSI Directive.

[159] Article 8.2 of the PSI Directive.

[160] See also Article 29 Data Protection Working Party 'Opinion 7/2003 on the re-use of public sector information and the protection of personal data - Striking the balance', WP83, 12 December 2003, p. 2, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp83_en.pdf.

The *legitimacy* principle requires, as indicated earlier, that one of the grounds provided in either art. 7 or 8 of the Directive must be present in order for the processing of personal data to take place.[161] For the initial collection of PSI constituting personal data, the legitimacy of processing must in principle be based on one of the following grounds:

- the processing is necessary for compliance with a legal obligation to which the controller is subject (art. 7, c DPD); or
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed (art. 7, e DPD).162

A task carried out by government administrations in the public interest is in principle only legitimate if it complies with the three basic principles of public law, namely its (1) legality (2) speciality and (3) proportionality.[163] Where the activity performed by the public sector body constitutes an interference in the private or family life of the individuals concerned, article 8, 2 of the European Convention of Human Rights similarly requires that such interference is:

- in accordance with the law (legality),
- necessary in a democratic society (proportionality), and
- in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (finality).164

Finally, a combined reading of articles 7, 8 and 52 of the EU Charter of Human Rights similarly requires that any interference in the private life and or right to the protection of personal data

---

161 Cf. *supra*; section 4.4.

162 See also FIDIS 16.1, *o.c.*, p. 36. The extent to which consent by the data subject alone can provide a legitimate basis for the collection of information by public sector can be questioned: in first instance, the requirement which states that the data subject's consent must be 'freely given' (art. 2, h DPD) will significantly restrict the number of instances in which consent could serve as the basis for the processing by public sector bodies. Second, even in instances where the citizen could arguable express a valid consent towards the processing, there is by no means an automatic exemption from the requirement of a clear regulatory framework. (Van Alsenoy B., Kindt, E. and Dumortier, J., 'Privacy and Data Protection Aspects of e-Government Identity Management', *l.c.*, p. 254. After all, public sector bodies may only act within the competences the law attributes them (principle of legality) (see also Article 29 Data Protection Working Party 'Opinion 7/2003 on the re-use of public sector information and the protection of personal data - Striking the balance', *l.c.*, p. 7.). Additional regulatory initiatives may therefore still be necessary depending on the application, in order to provide an adequate legal basis for collection.

163 De Bot, D., *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, *o.c.*, p. 37; FIDIS D16.1, *o.c.*, p. 36 et seq ; Van Alsenoy B., Kindt, E. and Dumortier, J., 'Privacy and Data Protection Aspects of e-Government Identity Management', *l.c.*, p. 254.

164 Regarding the question of whether the processing of personal data processing constitutes an 'interference' in the private or family life of the individuals concerned under art. 8 ECHR see *inter alia*: European Court of Human Rights, *Amann v. Switzerland*, 16 February 2000 (paragraph 65 et seq.); *Rotaru v. Romania*, 4 May 2000 (paragraph 43 et seq.); *Copland v. United Kingdom*, 3April 2007 (paragraph 43 et seq.), available at http://www.echr.coe.int/echr. For the purposes of our current analysis it is sufficient to point out that the large-scale and systematic collection (and subsequent processing) of personal data relating to citizens, such as that which takes place in the context of the creation and maintenance of population and other registers, constitutes an interference within the meaning of article 8 ECHR. As it is this type of information which is of primary interest in the context of INDI Services, our subsequent analysis is framed by the premise that the initial collection and subsequent processing of this information by public sector bodies must be in accordance with the requirements of legality, finality and proportionality.

must (1) be provided for by law (legality), genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others (finality) and be necessary to achieve these aims (proportionality).

According to the European Court of Human Rights, the requirement that an interference must be 'provided by law' (legality) refers to the law in its broad ('material') sense and is not strictly limited to statutes or acts. Such legal basis must however still be sufficiently precise to allow individuals to foresee its consequences and to give them adequate protection against arbitrary interference ('foreseeability test').[165]

The *finality* principle similarly requires that the controller clearly specifies the purposes of the processing.[166] Where the basis of the processing lies in a statutory provision, this provision must clearly determine the purposes for which the processing will take place. Absent such a clear specification, the statutory provision authorizing the processing would not only violate the principle of finality but would also fail the aforementioned foreseeability test.[167] Once specified, the use of personal data by the competent public sector body is in principle bound by this purpose. Directive 95/46/EC allows for 're-purposing' of personal data (i.e. re-use for a purpose which cannot be considered compatible with existing purpose) only if the envisaged processing in turn meet all the requirements the law ordinarily imposes upon data processing operations.[168] This implies treating the subsequent processing operation as an entirely "new" processing operation, which must meet all the requirements set forth by the Directive.[169] As a result, the re-use of PSI constituting personal data may only take place where:

- the processing may reasonably be considered as compatible with the existing specified purpose (as defined within the relevant jurisdiction); or
- in absence of such compatibility, there is a separate legal basis which specifically warrants the disclosure.

Although the Article 29 Working Party recognizes that consent could in principle provide a legitimate basis for the disclosure of PSI to third parties, a number of caveats must be made in light of the principle of *lawfulness* of processing (art. 6, a of Directive 95/46/EC). The specification that the processing must be conducted "lawfully" means that the data processing has to comply with all other laws and regulations.[170] If the processing infringes on a rule outside the Directive, the processing itself will also be considered unlawful. The statutory bases governing the collection and use of PSI may themselves prevent the disclosure of information even where the data subject has given her consent. For example, the access to data maintained in national citizen registries may be restricted to entities that have received explicit authorization either through a legal provision, or by means of an explicit authorization issued by the national

165 FIDIS D16.1, *o.c.*, p. 36 et seq. ; Van Alsenoy B., Kindt, E. and Dumortier, J., 'Privacy and Data Protection Aspects of e-Government Identity Management', *l.c.*, p. 254.

166 Cf. *supra*; section 4.6.

167 See also Article 29 Data Protection Working Party 'Opinion 7/2003 on the re-use of public sector information and the protection of personal data - Striking the balance', *l.c.*, p. 7.

168 De Bot, D., *o.c.*, p. 121 and Léonard, Th., 'La protection des données à caractère personnel et l'entreprise' ['The protection of personal data and the enterprise'], in X., *Guide juridique de l'entreprise* ['Legal guide for the enterprise'], Brussels, Kluwer, 2004, livre 112.1, p. 29. See also FIDIS D.16.1, *o.c.*, p. 37-39 and Van Alsenoy B., Kindt, E. and Dumortier, J., 'Privacy and Data Protection Aspects of e-Government Identity Management', in Van der Hof, S. and Groothuis, M.M. (eds.), *Innovating Government. Normative, Policy and Technological Dimensions of Modern Government*, Information Technology and Law Series, Volume 20, T. M. C. Asser Press, The Hague, The Netherlands, p. 255.

169 FIDIS 16.1, *o.c.*, 38.

170 De Bot, D., *Verwerking van Persoonsgegevens* ['Processing of Personal Data'], *o.c.*, 116.

data protection authority.[171] Reliance upon data subject's consent in such instances would arguably not be feasible, as it would circumvent these statutory restrictions and thereby violate the principle of lawful processing.[172] In addition, as already indicated, public sector bodies may only act within the competences the law attributes them (principle of legality).[173] It could therefore also be argued that administrative agencies who do not have a specific legal mandate for releasing personal data to third parties, even where the data subject has consented, would still be prohibited from doing so (due to a lack of authority).[174]

In light of the foregoing considerations, we may conclude that the re-use of personal data maintained by public sector bodies for purposes other than those laid down legal basis authorizing the processing is in principle prohibited. Consent of the data subject will not constitute a valid basis for the processing, except where (a) the processing may reasonably be considered as compatible with the existing specified purpose or (b) there is a specific legal basis which warrants the disclosure of the information on the basis of the consent of the data subject (with which the envisaged processing operation could be deemed compatible).

5.3 Implications

Where INDI Services wish to make use of personal data that is made available by public sector bodies for re-use, they will fall within the remit of the PSI Directive. This Directive creates a number of provisions aimed at ensuring the development of a level playing field for actors seeking to re-use PSI for commercial (or non-commercial) purposes. These provisions may in principle benefit INDI Operators as well as the other actors that play a role in the PIM ecosystem. Specifically, the PSI Directive will help ensure fair competition among these actors, in particular through:

- the prohibition of non-discrimination and exclusive arrangements;
- the transparency obligations of public sector in relation to the information they make available for re-use; and
- the restrictions concerning the conditions under which the PSI is disclosed.

5.4 Legal barriers and gaps

Despite the aforementioned benefits, there are still a considerable number of legal barriers and gaps towards the large-scale use of data maintained by public sector bodies in the context of INDI Services. These barriers and gaps all revolve around the same issue, namely the absence of

[171] This is for instance the case in Belgium, where access to the National Register requires prior authorization by a specific 'sectoral committee' of the DPA, except in instances where there is an explicit authorization in either a statute or royal decree. See D. De Bot, De Bot, D., *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, ['Privacy protection in e-government in Belgium. A critical analysis of the National Register, the Crossroadsbank for Enterprises and the electronic identity card'], Vandenbroele, Brugge, 2005, p. 132 et seq.

[172] See also *supra*; section 4.9.2.

[173] See also Article 29 Data Protection Working Party 'Opinion 7/2003 on the re-use of public sector information and the protection of personal data - Striking the balance', *l.c.*, p. 7.

[174] At the same time we must note that in certain instances the laws of the Member State might oblige the disclosure of personal data towards third parties (e.g., in laws regulating public property registers). (*Ibid*, 8).

a regulatory framework which enables and promotes the re-use of PSI pursuant to a data subject request.

A first gap concerns the absence of an obligation for Member States to make their documents available for re-use. Only if Member States (or their public bodies) choose to do so, will they have to comply with the obligations of the PSI Directive and the transposing national legislation. This entails that in many Member States the default rule may be that the data maintained by public sector bodies will not be made available to INDI Operators or INDI Services.

In addition to the lack of an obligation to make available PSI, a number of legal barriers result from the restrictions contained in Directive 95/46/EC and article 8 of European Convention of Human Rights. The principle of legitimacy, together with the principle of lawfulness, in practice requires that the basis for the processing must be provided by law. The finality principle in turn entails that the legal basis authorizing the processing must clearly determine the purposes for which the processing will take place. It may be expected that in many instances the purposes for which the user is requested to make available PSI relating to her will not match the purposes for which the data is being processed by the public sector body. In such instances even the consent of the data subject will not constitute a valid basis for the processing of these data, except where there is a specific provision which warrants the disclosure of the information on the basis of data subject consent (or otherwise authorizes the disclosure). Finally, consideration must also be given to the fact that statutory bases governing the collection and use of PSI may themselves prevent the disclosure of information even where the data subject has given her consent.

While taking note of these restrictions as potential obstacles, it is also important to consider that they were adopted to protect specific interests, often those of the data subjects themselves. When assessing these obstacles from a policy perspective, one should carefully consider these interests, and whether or not an envisaged derogation might risk eroding the protection currently provided in the jurisdiction at hand.

5.5 Practical barriers

While the PSI directive has had a positive influence on the availability of PSI on the market, many practical barriers still need to be overcome. While changes in legislation may take away or reduce some of the barriers, many issues require a more comprehensive approach, whereby practical measures, policy development and efforts to change the mindset of the public sector need to go hand in hand.

The main barrier that remains is the general lack of awareness of the public sector about the benefits and risks of opening up their data for use by the private sector, civil society or the citizens. Public bodies are confronted with direct requests or more indirect calls for opening up their data (e.g. in the press), but they are not equipped with the tools and guidance they need to answer these requests. They feel that the data they have collected for their internal purposes does not have much value for the outside world, or they are worried that the data is of insufficient quality to be disseminated or that the data might be misused or misrepresented harming their reputation.[175] In addition, they often do not receive much support or guidance from central government in the adaptation of their functioning and internal procedures to incorporate the concepts of the PSI directive in their daily activities. Whether due to lack of resources or lack of

[175] Fioretti, M., *Open Data Open* Society, 2010 http://www.lem.sssup.it/WPLem/odos/odos.html (last accessed on 20 February 2011); De Vries M., , "Integrating Europe's PSI re-use rules – Demystifying the maze", *Computer Law & Security Review 27,* 2011, 69.

vision, governments of some of the EU Member States were satisfied with just transposing the PSI directive into national law, without attaching an actual implementation policy, guidelines or practical measures to the transposition. In this way, the PSI legislation remained a dead letter, leaving the public bodies to their own devices in developing an information policy to deal with re-use, and expecting the possible re-users to discover for themselves that public sector data might be available and useful for their plans. While some of the public bodies have risen to the challenge and developed a re-use policy, others remain in blissful ignorance about the enormous resources they hold.

6 E-Commerce

6.1 Directive 2000/31/EC

Directive 2000/31/EC[176] was adopted with the aim of establishing a clear and general framework for certain legal aspects of electronic commerce within the internal market.[177] This Directive, commonly referred to as the 'E-Commerce Directive', has mainly two objectives. In first instance it seeks to remove certain legal obstacles which were seen as hampering the development of electronic commerce within the internal market.[178] At the same time it is also aimed at providing legal certainty and ensuring consumer confidence towards electronic commerce.[179]

The E-Commerce Directive was proposed by the Commission in 1998 and signed by the Parliament and the Council in June 2000. Member States had time until January 2002 to implement the Directive in their national legal order.

The E-Commerce Directive regulates several aspects of information society services including freedom of services, the treatment of electronic contracts, and liability issues, among others. After elaborating upon the scope of this Directive, we will discuss those provisions which are most relevant for the deployment of INDI Services.

6.2 Scope

The E-Commerce Directive applies to "information society services", which have been defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' (see art. 2, a E-Commerce Directive)[180]. The notion of "information society services" covers a wide range of services. Many of the economic activities which take place online fall under the scope of the E-Commerce directive.[181] The key elements in determining whether or not a particular service can be qualified as an information society services are:

- remuneration;
- at a distance;
- by electronic means; and
- at the individual request of a recipient.

The element of remuneration does not necessarily refer to the specific way in which the service is financed, but rather that it refers to the existence of an economic activity or an activity for which

[176] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *O.J.* 17 July 2000, L 178/1-16.
[177] Recital (7) of Directive 2000/31/EC.
[178] Recital (5) of Directive 2000/31/EC.
[179] Recital (7) of Directive 2000/31/EC.
[180] This provision refers back the definition in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC.
[181] Recital (18) of the E-commerce Directive.

an economic consideration is given in return.[182] Information society services are therefore not restricted to services which are remunerated by their recipients as such.[183]

The element "at a distance" simply means that the parties are not simultaneously physically present in the same particular place.[184]

A service is "provided by electronic means" when the service is sent initially and received at its destination by means of electronic equipment for the processing (which includes digital compression) and the storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means.[185] This means that the service should be also sent and received with the use of electronic equipment. This requirement excludes the traditional distance selling methods, like mail-ordering, from the scope of this definition.[186]

"At the individual request of a recipient of services" means that the service is provided through the transmission of data on individual request.[187] Visiting a website is considered to be a service on demand, since the recipient 'requests' the website when typing the URL or following a link.[188]

Examples of information society services may include (in so far as they represent an economic activity): on-line contracting, services providing transmission of information via communication networks, services providing access to a communication network, hosting of information, services providing search tools, etc.[189]

The E-Commerce Directive also excludes a number of services and legal issues from its scope, among which:

- questions covered by the Data Protection Directive (art. 1 (5), b);
- questions relating to agreements or practices governed by cartel law (art. 1 (5), c);
- the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority (art. 1 (5), d).

[182] Any type of economic activity present will suffice, for example the costs of the service could be also covered by advertisement. (Lodder A., 'Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, in Lodder A. and Kasspersen (eds.), *eDirectives: Guide to European Union Law on E-commerce – Article by Article Comments*, Kluwer Law international, 2002, p. 71.)

[183] Recital (18) of the E-commerce Directive.

[184] See art. 1, 2 of the Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations (O.J. L 217/18-26).

[185] See art. 1, 2 of Directive 98/48/EC. It is not required that every aspect of the overall service that is being provided takes place by electronic means; nor that the final service consists of an immaterial good. See e.g. European Court of Justice, Case C-108/09, *Ker-Optika Bt. v ÀNTSZ Dél-dunántúli Regionális Intézete*, 2 December 2010 (applying Directive 2000/31/EC to the sale of contact lenses via the internet).

[186] Lodder, A., *l.c.*, p. 71.

[187] Art. 1, 2 of Directive 98/48/EC.

[188] Lodder, A., *l.c.*, p. 71.

[189] Recital (18) of the E-commerce Directive.

6.3 Internal market

Article 3 of the E-Commerce Directive aims to promote the free movement of information society services within the EU. It is comprised of two elementary principles, namely the rule of origin principle and the principle of freedom of services.

6.3.1 Country of origin

Article 3, 1 states that Member States must apply its national provisions to the providers of information society services established on its territory (insofar as this legislation falls within the 'coordinated field'[190]). The rationale for this provision is found in recital (22), which indicates that 'information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives'. The protection offered by a Member State should be provided not only to citizens of one state, but to all citizens of the European Community. Therefore the (primary) responsibility of enforcement and oversight is assigned to the competent authorities of the country where the service originates from, in order to improve the mutual trust among the Member States.[191]

6.3.2 Freedom of services

Article 3, 2 specifies that Member States 'may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State'. This provision entails that each Member State should in principle recognize the protection offered by the legislation of another Member State (falling within the co-ordinated field) as being adequate, and may not prevent an information society service provider from offering services within its jurisdiction for reasons related to the co-ordinated field.

The combined result of these two provisions is that every Member State must in principle allow information society service providers that are established in another Member State to provide their services within its territory. While this principle may seem straightforward, there are a number of important exceptions. First, the annex of the Directive enumerates a number of fields for which the provisions of art. 3 do not apply. In addition, Member States may impose restrictions on the provisioning of a given information society service where such restrictions are necessary for reasons of public policy (e.g., prevention, investigation, detection and prosecution of criminal offences), the protection of public health, public security or the protection of

[190] The 'coordinated field' is defined by article 2 (h) as requirements laid down in Member States' legal systems applicable to information society service providers or information society services (regardless of whether they are of a general nature or specifically designed for them). It concerns requirements with which the service provider has to comply in respect of (i) the taking up of the activity of an information society service, such as requirements concerning qualifications, authorization or notification and (ii) the pursuit of the activity of an information society service, such as requirements concerning the behavior of the service provider, requirements regarding the quality or content of the service, including those applicable to advertising and contracts, or requirements concerning the liability of the service provider.

[191] This provision should not be interpreted as meaning that the provider of information society services shall only be subject to the national laws of the Member State where it is established. Article 1 (4) of the Directive clearly indicates that the E-Commerce Directive 'does not establish additional rules on private international law nor does it deal with the jurisdiction of Courts'. As a result, information society service providers will still need to comply with the legislation of other Member States where their activities are subject to their legislation pursuant to international private law.

consumers (art. 3, 4).[192] These derogations must be taken into account in addition to the scope exemptions related to the 'coordinated field' (see art. 2 (h)).

6.4 No prior authorization

The provisioning of information society services may in principle not be made subject to prior authorization 'or any other requirement having equivalent effect' (art. 4). Prior authorization schemes which are not specifically and exclusively targeted at information society services are not affected by this provision.[193]

6.5 Transparency

Directive 2000/31/EC contains several information obligations for the providers of information society services:

- a general information obligation (art. 5);
- information to be provided in commercial communications (art. 6);
- information to be provided in relation to the conclusion of the contract as well as contract terms and conditions (art. 10); and
- information obligations relating to order placement (art. 11).

The general information obligation contained in article 5 requires the service provider to clearly identify himself. This includes making available information about his name, geographic address of his establishment, his email address, the trade register in which the service is entered and his registration number, any relevant supervisory authority (where applicable), and his VAT identification number. This information should be easily, permanently and directly accessible to both consumers and supervisory authorities. This means that it must be possible to obtain the information without much effort (easily) or additional acts (directly) like for example exploration of numerous site's web pages.[194] The objective behind this provision is to ensure transparency to acquire users' confidence, and to make the provider more reachable.[195] If the service refers to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they include tax and delivery costs (Article 5(2)).

These transparency obligations apply in addition to the information obligations established through other Community instruments, like for example the 97/7/EC Directive on the Protection of Consumers in Respect of Distance Contracts[196] or Directive 95/46/EC[197].

---

[192] Article 3 provide for a notification and evaluation procedure which must be followed where a Member State wishes to derogate from the principle of freedom of services provided in art. 3, 2.

[193] Art. 4, 2 additionally provides a specific exception for prior authorization schemes which are covered by Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorisations and individual licences in the field of telecommunications services.

[194] Lodder, A., *l.c.*, p. 77.

[195] Finocchiaro G., 'Directive 2000/31/EC –Directive on electronic commerce', in Bullesbach A., Poullet Y., Prins C. (eds.), *Concise European IT Law*, Kluwer Law International Alphen aan den Rijn, 2005, p.233.

[196] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, *O.J.* 4 June 1997, L 144/19–27. This Directive is often also referred to as the 'Distant Selling Directive'. Art. 4 of this Directive for instance requires that, prior to the conclusion of any distance contract, the consumer shall be provided with the following information: (a) the identity of the supplier and, in the case of contracts requiring payment in advance, his address; (b) the main characteristics of the goods or services; (c) the price of the goods or services

6.6 Contracts concluded by electronic means

The E-Commerce Directive requires Member States to ensure that contracts concluded by electronic means are allowed in their legal regime. Specifically, they need to ensure that the legal requirements applicable to the contractual process do not create obstacles for the use of electronic contracts nor result in depriving such contracts of legal effectiveness and validity on account of their having been concluded by electronic means(article 9(1)). The Directive does, however, leave room for the Member States to exclude certain types of contracts from the scope of this article (article 9 (2)).[198]

The section on electronic contracting also includes specifications on the information to be provided – complementing the other information requirements - and on order procedures (articles 10 and 11). Pursuant to the former category of requirements, the service providers must provide the users with information on (a) the technical steps necessary to conclude the contract, (b) the filing and accessibility of the contract (c) the identification and correction of input errors and (d) the language of the contract. The listed information must be given prior to the order being placed. The aim of the article is to ensure the transparency of the contractual process, which is crucial especially in consumer contracts.[199] The latter category of requirements addresses the issue of placing of the order. In cases where the recipient of the service places his order through electronic means the service provider should acknowledge the receipt of the order without undue delay. Such acknowledgment of receipt may in principle take a form of online provision of the service purchased.[200] A second part of the provision stipulates that the order and acknowledgement are deemed to be received at the moment parties are able to access them. This

including all taxes; (d) delivery costs, where appropriate; (e) the arrangements for payment, delivery or performance; (f) the existence of a right of withdrawal, except in the cases referred to in Article 6 (3); (g) the cost of using the means of distance communication, where it is calculated other than at the basic rate; (h) the period for which the offer or the price remains valid and (i) where appropriate, the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently.

197 Cf. *supra*; section 4.9.1.

198 Article 9 (2) states that Member States may provide that the rule of art. 9 (1) shall not apply in relation to (a) contracts that create or transfer rights in real estate, except for rental rights; (b) contracts requiring by law the involvement of courts, public authorities or professions exercising public authority; (c) contracts of suretyship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession; (d) contracts governed by family law or by the law of succession.

199 Cool Y., Montero E., 'Directive 2000/31/EC –Directive on electronic commerce', in Bullesbach A., Poullet Y., Prins C. (eds.), *l.c.*, p. 243.

200 See recital (34). One could argue that if service provisioning occurs immediately after the order has been placed, that this provisioning provides implicit (yet sufficient) acknowledgement of the receipt of order. However, when reading recital (34) in its entirety, and in combination with the subsequent recitals, it would appear that this phrase merely provides a clarifying statement as to the margin Member States have in implementing this particular aspect of the Directive. This reading implies that Member States would actually need to incorporate a provision to such an extent in their national legislation when implementing the Directive, or that the national implementation should at a minimum allow for such an interpretation. In absence of such a provision, information society service providers would still be required to send the recipient of the service an explicit confirmation of their order, even where service provisioning takes place on-line immediately after the order has been placed.

means that the message is considered to be received as soon as it arrives at the mail server, and the question whether the recipient of the email took notice of it is not relevant.[201].

6.7 Liability of intermediaries

Section 4 of the e-Commerce Directive regulates the liability of intermediary service providers. The Directive provides that intermediary service providers shall not be liable for actions that qualify as 'mere conduit' (article 12), 'caching' (article 13) or 'hosting' (article 14). In order to benefit from these exemptions, the providers of such services must comply with the conditions foreseen by each article. The rationale behind these provisions was the concern that if intermediaries were to be held liable for third party content on similar grounds as 'publishers' or 'distributors', it could restrain service providers from entering the market.[202]

The scope of these exemptions has a horizontal nature, which means that they cover various types of illegal content (infringements on copyright law, defamation law, protection of minors, privacy law, unfair commercial practices, etc.) and different kinds of liability (criminal, civil, direct, indirect).[203]

Before we discuss the exemptions in greater detail, it is important to note that if the conditions for being exempt are not met, this does not mean that the intermediary is per se subject to liability. Such a determination would still need to be made in light of the conditions for imposing liability under the national law(s) applicable to the case.[204]

6.7.1 Mere conduit

The first exemption of liability concerns intermediary service providers that act as a 'mere conduit' (art. 12). This exemption is aimed at two types of information society services:

- those services which consist of the transmission in a communication network of information provided by a recipient of the service ('transmission services'); and
- those services which consist of the provision of access to a communication network ('access services').

The 'mere conduit' exemption of liability only applies if the service provider:
(a) did not initiate the transfer of data[205];
(b) does not select the recipient of the data; and
(c) does not select or modify the transmitted data.[206]

---

[201] Lodder, A., *l.c.*, p. 86. This solution resembles the one proposed in the UCITRAL Model Law on Electronic Commerce introduced by the United Nations in 1996 (see Article 15 of The Model Law: http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf) (*Ibid*, 86.).

[202] Walden I, in: Bullesbach A., Poullet Y., Prins C. (eds.), *l.c.*, p. 248.

[203] Helberger N., et al., 'Legal Aspects of User Created Content' in IDATE, TNO, IViR, *User-Created Content: Supporting a Participative Information Society*, Study for the European Commission (DG INFSO), December 2008, available at http://www.ivir.nl/publications/helberger/User_created_content.pdf.

[204] Jakobsen, S.S., 'Mobile Commerce and ISP Liability in the EU', *International Journal of Law and Information Technology* 2010, vol. 19 no. 1, p. 38.

[205] This exemption is quite logical: if such initiative existed, the service provider would not be able to claim that his role is limited to that of an intermediary.

Recital (42) further stipulates that the exemptions provided by the Directive apply only to cases 'where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network'.[207] It further elaborates that such activities are of mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

The liability exemption for mere conduit also extends to the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission (art. 12, 2). The services mentioned in art. 12 could be compared to postal services, which are similarly not held liable for the illegal content of a letter.[208]

Despite the lack of liability of the service provider, there still exists a possibility of directing prohibitory injunctions towards a 'mere conduit' intermediary. A court or administrative authority may order the service provider to terminate or take measure to prevent a particular infringement where the legal system of the Member State provides for this (Article 12 (3)).

Given the various restrictions associated with this exemption, it is expected that none of the actors involved in the provisioning of INDI Services (Users, Operators, Data Sources, Relying Parties) will qualify for this exemption under the Directive.[209]

6.7.2 Caching

The second liability exemption provided by the E-Commerce Directive concerns 'caching' of information. Caching is described as 'the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request'. This exemption only concerns information society services which consist of the transmission in a communication network of information provided by a recipient of the service ('transmission services') (art. 13, 1).

---

[206] This requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission (recital (43)).

[207] While recital (42) purports to address all of the exemptions of the Directive, one might argue that the scope of this part of the recital should be limited to the transmission and access services identified in articles 12 and 13. After all, the exemption for hosting identified in art. 14 does not limit its scope to either transmission or access services. See also Montéro, E., 'Les responsabilités liées au web 2.0', *Revue du Droit des Technologies de l'Information* 2008, n° 32, p. 367. However, the ECJ has held recital (42) equally applicable to hosting services: see European Court of Justice, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.), paragraphs 113-114.

[208] See Lodder, A., *l.c.*, p.87

[209] Despite the functional nature of the criteria set forth by art. 12, the result of its conditions is that in practice the exemption only benefits a limited group of service providers such as telecommunications operators and ISPs. However, certain Member states have, in the implementation of the E-Commerce Directive, extended the scope of their national laws to cover services provided by other intermediaries e.g., search engines. See Verbiest T. et al., *Study on the Liability of Internet Intermediaries*, commissioned by the European Commission, 12 November 2007, p.4, 19, available at: http://ec.europa.eu/internal_market/e-commerce/directive_en.htm#firstreport.

When comparing the caching exemption with the exemption for transient storage under the 'mere conduit' rule of art. 12, 2 (cf. supra), the wording appears to be very similar. Both refer to the 'automatic, intermediate and temporary storage' of information provided by the recipient of the service. However, there are several notable differences in scope among the exemption of art. 12, 2 and that of art. 13, 1:

- the 'caching exemption' only applies to transmission services (and formally does not extend to access services)[210];
- whereas the mere conduit exemption for transient storage is aimed at storage which takes place for the *sole purpose of carrying out the transmission*; the caching exemption concerns storage which is performed *for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request.*[211]

The key difference between the caching exemption for transient storage and the exemption for transient storage under the mere conduit provision therefore appears to be the purpose for which the storage is taking place.[212]

Like the 'mere-conduit' exemption, the information society service provider shall only be exempted from the liability under Directive if he is in no way involved with the information transmitted (recital (43)). In addition, the following five conditions must be met in order to benefit the caching exemption (art. 13, 1). First of all, the (service) provider may not modify the information as it would deprive him of the position of the intermediary. Second, the provider has to comply with conditions on access to the information.[213] Third, the provider must update the information regularly in accordance with the generally recognized rules and practices in this area. Fourth, the provider may not interfere with the lawful use of technology that is used to measure the use of information.[214] Finally, in order to benefit from the exemption the provider must remove the cached information immediately upon obtaining actual knowledge that the initial source of the information is removed, access to it has been disabled, or that a court administrative authority have ordered such removal or disablement.

The liability exemption for caching in no way affects the possibility for Member States to provide for the possibility of prohibitory injunctions (art. 13 (2)).

---

[210] We must note that the exemption of art. 12, 2 also pertains to the activity of transmission rather than access provisioning. However, due to the differences in structuring of the respective provisions, it would appear that strictly speaking only information society services which qualify as transmission services benefit from art. 12, 3, whereas both transmission services and access services are able to avail themselves of art. 12, 2.

[211] Based on this consideration, doctrine has concluded that the 'transient storage' under art. 13, 1 could be longer than the storage envisaged by art. 12, 2 (see Lodder, A., *l.c.*, p. 88).

[212] An example of the former would be the storage involved in "packet switching transmission" performed by ISP's; whereby information is stored for shorter period of time in small pieces (see Baistrocchi, P.A., 'Liability of intermediary service providers in the EU Directive on Electronic Commerce', *Computer & High Technology Law Journal* 2002, vol. 19, 119. An example of the latter is the server or proxy caching performed by ISP's, whereby they conduct automatic, intermediate and temporary storage of popular websites in order to speed up the users access to the website (see Jakobsen, S.S., *l.c.*, 43).

[213] This provision implies that the conditions on access to the original data should be respected for the cached copies as well. For instance, if the original party posting the information applies certain conditions to access such as the payment of a subscription fee, the cached information may not be made available free of charge (see Baistrocchi, P.A., l.*c.*, 121 and Lodder, A., *l.c.*, p. 88).

[214] This would occur for example when technologies to keep track of the number of users visiting a web page showed less hits because of the caching activity (Lodder, A., l.*c.*, p. 88).

Here too it would appear that none of the actors involved in the provisioning of INDI Services (Users, Operators, Data Sources, Relying Parties) will qualify for this exemption under the Directive.

6.7.3 Hosting

Article 14 of the E-Commerce Directive provides that where an information society service consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored (at the request of a recipient of the service), on the condition that:

- the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

This provision exempts 'hosting' service providers of liability for the information that they store (provided the conditions set forth by art. 14 are met). The storage by these service providers differs from the storage carried out in the context of mere conduit or caching serves mainly in terms of the purposes for which the storage takes place. In contrast to mere conduit or caching services, such storage is not merely 'incidental' to the provision of the transmission or access services.[215] Storage may be provided for a prolonged period of time, and may also be the primary object of the service.[216]

The (de facto) obligation for the hosting provider to 'act expeditiously' to remove or to disable access to this information once he has become aware of the illegality of the information, has been commented extensively.[217] The provision is seen as creating 'an incentive to systematically take down material, without hearing from the party whose material is removed, thus preventing such a party from its right to evidence its lawful use of the material'.[218] A dilemma arises for the service providers who could face the responsibility for not removing the information, or, on the other hand, they could be held liable by the recipient of the service for wrongfully removing the

[215] Walden I, in: Bullesbach A., Poullet Y., Prins C. (eds.), *l.c.*, p. 253.

[216] It has been said that this exemption was originally aimed at ISP's providing space on their internet servers for third parties' websites, or bulletin boards or chat room services provided by the ISP itself (where the ISP only provides technical means for the users' communication without interfering with the content being communicated between the users) (Jakobsen, S.S., *l.c.*, 44). However, the exemptions provided by the E-Commerce Directive are defined in functional terms (i.e. in terms of the activity being performed), not in terms of the qualification of the actor. While the European legislator arguably only envisioned providers whose services consisted mainly, if not exclusively, in the performance of operations of a strictly technical nature, the scope of the exemption may also be applied to other entities (provided the conditions set forth by art. 14 are met). As a result, the exemption may in principle benefit any type of service provider who stores content at the request of the recipient; including so-called 'web 2.0' service providers (see Montéro, E., *l.c.*, 369-373).

[217] See Lodder, A., *l.c.*, p.89 ; Julià-Barceló, R. and Koelman, K., 'Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough', *Computer Law & Security Report* 2000, vol. 4, pp. 231-239; Holmes, S. and Ganley, P., 'User generated content and the law', *Journal of Intellectual Property Law & Practice* 2007, p. 338, 340.; Yakobson, M., 'Copyright Liability of Online Service Providers After the Adoption of the E.C. Electronic Commerce Directive: A Comparison to U.S. Law', *Entertainment Law Review* 2000, p. 144, 148 et seq.

[218] Julià-Barceló, R. and Koelman, K., *l.c.*, p. 231.

material.[219] Recital 46 of the Directive states that 'the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level'. However, the Directive does not provide more detailed rules on how the procedure should be handled by service providers. More specifically, there is no indication on how to assess whether the notices of illegality are reliable enough to act upon.[220] Member States are given a possibility to establish specific requirements that must be fulfilled expeditiously prior to the removal or disabling of information (Article 14(3)). This opportunity, however, has not been widely taken up by the EU countries.[221]

The exemption of art. 14 additionally does not apply when the recipient of the service is acting under the authority or the control of the provider (art. 14, 2). For example, if the service provider is acting as an employer or supervisor of the service recipient, it will not qualify for the exemption if the content was introduced pursuant to its instructions.[222]

Finally, article 14 foresees the same possibility to introduce prohibitory injunctions as the articles on mere conduit and caching.

The extent to which the actors involved in the provision of INDI services shall be able to avail themselves of the hosting exemption appears to be limited, as many of the actors will exert a considerable amount of control over the data they process. The INDI operator might however be an exception in this regard. The ECJ has held the hosting exemption to be applicable to 'referencing service providers', provided that service provider

> "*has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned*".[223]

The question arises to what extent these consideration might be applied analogously to an INDI Operator. Depending on the implementation, an INDI Operator might be able to avail himself of the hosting exemption for the references to identity data it maintains. Where the role of the INDI Operator is merely 'passive' (e.g., limited to storing and making available references to identity information maintained by a Data Source), without having knowledge or control over the information stored at the request of the User or Data Source, it would appear that it might be able to avail itself of the hosting exemption. However, where the role of the INDI Operator is such that knowledge or control over the transmitted information may be attributed to the Operator, the exemption will not apply.

---

[219] Lodder, A., *l.c.*, p. 89.

[220] Julià-Barceló, R. and Koelman, K., *l.c.*, p. 231. The solution proposed by the Directive resembles the 'notice and take down' procedure of the US Digital Millennium Copyright Act. The American solution, however, introduces a set of formal requirements and a minimal content for the notices. Moreover, the DMCA includes also a 'put back' procedure, which gives an opportunity to recipients of the service to defend themselves in case the material is in fact legal. (Lodder, A., *l.c.*, p. 89.)

[221] Julià-Barceló, R. and Koelman, K., *l.c.,* p.238.

[222] Lodder, A., *l.c.*, p. 89.

[223] European Court of Justice, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.), paragraph 120.

6.7.4 No general obligation to monitor

Article 15 states that Member States may not impose a general obligation on providers, when providing the services covered by article 12, 13 and 14 (i.e. mere conduit, caching or hosting) to monitor information they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.

The prohibition towards monitoring obligations refers solely to monitoring obligations of a general nature. In other words, it does not concern monitoring obligations in a specific case, nor does it affect orders by national authorities in accordance with national legislation.[224] The Directive also does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.[225]

The prohibition of general monitoring schemes only concerns the instances in which the service provided qualifies as a mere conduit, caching or hosting service. Therefore in instances where the service provided does not meet all the conditions to be qualified as either a mere conduit, caching or hosting service, Member States are in principle still free to institute general monitoring obligations.[226]

Article 15 (2) defines two additional obligations which Member States may impose upon information society service providers. Member States are provided with a possibility to require such providers to inform the authorities of alleged illegal activities or illegal information provided by recipients. Such notification would then need to be given as soon as the provider becomes aware of the illegal activity. Member States may also establish obligations on providers to disclose the identity of recipients with whom they have storage agreements.

6.8 (Voluntary) Codes of conduct

In order to help remove barriers to the development of cross-border services within the European Community, art. 16 of the E-commerce Directive provides that both the Member States and the Commission are encouraged to draw up codes of conduct at the Community level.[227] These codes would be designed to contribute to the proper implementation of the general obligations of information society service providers under the E-commerce Directive, and would apply to particular trades or professional or consumer associations and organizations (art. 16, 1).

---

[224] Recital (47). In other words, the E-Commerce Directive only prohibits general monitoring obligations, but does not restrict the ability for national authorities to impose 'specific' monitoring obligations. In practice it may however be difficult to distinguish between the two. (See Montéro, E., *l.c.*, p. 384-386)

[225] Recital (48). This prohibition towards general monitoring obligations in other words does not dispense information service providers of any obligations of due diligence which might be incumbent on them pursuant to national legislation (as long as such obligations do not amount to a general monitoring obligation). For instance, the provider of an on-line service might be expected to adopt appropriate restrictions in its terms of use, putting in place a complaint or other notification mechanisms to identify illegal content. However, such general obligations are in principle independent of the potential liability of service providers for the content itself (see Montéro, E., l.*c.*, 382-383).

[226] See Jakobsen, S.S., *l.c.*, 43.

[227] S. Callens, "Telemedicine and the E-commerce Directive", *European Journal of Health Law* 2002, 101.

The recitals of the Directive clearly provide that these codes are voluntary in nature and that the interested parties are free to decide whether or not they adhere to such codes.[228]

Nevertheless, such codes can be very useful to ensure full compliance with other rules that apply to particular professions, trades and organizations. These codes can for instance determine the types of information that can be given for the purposes of commercial communications in conformity with the rules that apply to a particular group.[229]

6.9 Implications

It may be expected that the provisioning of INDI services shall qualify as information society services and will therefore fall within the remit of the E-Commerce Directive. This implies that service providers such as the INDI Operator shall in principle benefit from the internal market provisions established by the Directive; the general prohibition of a prior authorization scheme (to which significant exceptions exist); as well as the provisions on electronic contracting. It also implies that these actors will have to comply with the substantive requirements set forth by this Directive, such as the transparency obligations set forth in articles 5, 6 10 and 11.

As far as the liability regime established by the E-Commerce is concerned, it appears as if few of the actors in the PIM ecosystem currently envisioned by GINI shall be able to avail themselves of the exemptions set forth by articles 12-14 (although their (non-) applicability will depend on the actual implementation). Notable exception in this regard is the INDI Operator, who might be able to avail itself of the hosting exemption, provided it has 'not played an active role of such a kind as to give it knowledge of, or control over, the data stored'.[230]

The liability of actors involved in the PIM Ecosystem will therefore mainly be determined by other areas of regulation. The most relevant EU instrument in this regard appears to be Directive 95/46/EC, which provides that controllers shall be liable for damages incurred from unlawful processing (art. 23).[231]

[228] Recital (49) E-Commerce Directive.

[229] See S. Callens, "Telemedicine and the E-commerce Directive", *l.c.*, 101.

[230] European Court of Justice, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.), paragraph 120.

[231] Art. 23 (2) provides that a controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

7 E-Signatures

7.1 Directive 1999/93/EC

Directive 1999/93/EC[232] establishes a legal framework for electronic signatures and certain certification-services. This Directive, commonly referred to as the 'E-Signature Directive', seeks to facilitate the use of electronic signatures and to contribute to their legal recognition within the internal market.[233] Specifically, it aims to remove barriers resulting from divergent national rules with respect to the legal recognition of electronic signatures and the accreditation of certification-service providers.[234] It also seeks to increase confidence in, and general acceptance of, new technologies by establishing a clear Community framework regarding the conditions applying to electronic signatures.[235]

The E-Signature Directive was proposed by the Commission in October 1998 and signed by the Parliament and the Council in December 1999. Member States had time until July 2001 to implement the Directive in their national legal order.

While at first glance the extent to which 1999/99/EC is directly relevant to the deployment of INDI Services may appear limited, we nevertheless consider it worthwhile to elaborate upon this regulatory framework. As already indicated, one of the key objectives of GINI is to allow users to link their INDI space with authoritative identity data maintained by both public- and private-sector entities. Once such a connection has been established, the user would be able to present links to this information to other parties to corroborate her identity and/or other attributes. This model bears a strong resemblance, at least intuitively, to third-party certification models. As will become apparent over the following sections, the third-party certification model also underlies many of the provisions of the E-Signature Directive.

7.2 Scope

The E-Signature Directive regulates several aspects of the recognition of electronic signatures and related certification-services and products. The E-Signature Directive recognizes three types of electronic signatures:

1. 'Ordinary' electronic signatures, which are defined as any data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication (art. 2, 1);

2. 'Advanced' electronic signatures, which are defined as electronic signatures which meet the following requirements (art. 2, 2):

---

232 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *O.J.* 19 January 2000, L 13/12-20.
233 Article 1 of Directive 1999/93/EC.
234 Recital (4) of Directive 1999/93/EC.
235 Id.

a) they are uniquely linked to the signatory;
b) they are capable of identifying the signatory;
c) they are created using means that the signatory can maintain under their sole control; and
d) they are linked to the data to which it relates in such a manner that any subsequent change in the data is detectable.

3. 'Qualified' electronic signatures, which can be described as advanced electronic signatures which are:
   a) based on a qualified certificate (see annex I) provided by a certification service provider who fulfills the requirements laid down in annex II (art. 2, 10); and
   b) created using a secure signature-creation device (SSCD) (meeting the requirements set forth in Annex III) (see art. 5, 1).

In addition to setting forth rules related to the recognition of the aforementioned e-signatures, the Directive also contains several provisions governing the provisioning of certification-services. A 'certificate' is defined by art. 2, 9 as 'an electronic attestation which links signature-verification data to a person and confirms the identity of that person'.[236] A 'certification-service-provider' (CSP) is in turn defined as 'an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures' (art. 2, 11).[237]

An 'electronic-signature product' is defined by art. 2, 12 as 'hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures'.

The E-Signature Directive also explicitly several matters from its scope. It does not cover aspects related to[238]:

- the conclusion and validity of contracts; or
- requirements as regards form or performance of contracts; or

[236] Signature-verification data is in turn defined as 'data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature' (art. 2, 7). A typical example of the certificates envisioned by art. 2 (9) are the public-key certificates issued by a Certification Authority (CA) in a Public-Key Infrastructure (PKI) (through which the CA attests to the relationship between the identified entity and the public verification key identified in the certificate). (X. Huysmans and B. Van Alsenoy (eds.), 'D1.3 Conceptual Framework – Annex I. Glossary of Terms', v1.07, report for the IBBT project IDEM, 17 December 2007, p. 11 available at https://projects.ibbt.be/idem/uploads/media/2007-12-27.idem.glossary.v1.07.pdf)

[237] The rationale for this relatively broad definition of certification-service providers can be found in recital (9) of the Directive, which states that 'e[lectronic] signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, timestamping services, directory services, computing services or consultancy services related to electronic signatures'. See also Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P., 'The legal and market aspects of electronic signatures – Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EAA, the Candidate and the Accession Countries', Study for the European Commission within the eEurope 2005 framework, 2003, p. 34, available at http://ec.europa.eu/information_society/policy/esignature/docs/electronic_sig_report.pdf.

[238] See art. 1, recital (17) and (21) of Directive 1999/93/EC.

- rules and limits governing the use of electronic documents and electronic signatures.

7.3 Legal effects of electronic signatures

Article 5, 1 of the E-Signature Directive obliges Member States to ensure that qualified electronic signatures:

a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
b) are admissible as evidence in legal proceedings.

The result of this provision is that a qualified electronic signature must in principle be given the same legal effect as a handwritten signature in relation to a paper document.[239] The E-Signature Directive does not exclude that other types of electronic signatures be given legal effects, on the contrary: article 5, 2 provides that Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service provider, or
- not created by a secure signature-creation device.

In other words, the general principle of legal recognition applies to all three types of electronic signatures.[240] Article 5, 2 entails that a denial of legal effect of a particular electronic signature must be based on other considerations than the elements enumerated by art. 5, 2. As a result, a denial of legal effect will typically require a substantive disapproval of the particular technology involved, e.g. by finding it lacks technological reliability.[241]

The combined result of these provisions is that electronic signatures should be given the same legal effect as handwritten signatures provided that they offer 'functionally equivalent' safeguards. Whether or not this is the case is, in principle, a matter of judicial consideration, to be determined in light of the facts of the case and the relevant national law defining the requirements for handwritten signatures. For one type of electronic signatures the European legislator imposes a finding of equivalency, namely in the case of qualified electronic signatures. But even where these requirements are not met the Directive stipulates that an electronic signature should not be dismissed merely due to its electronic nature.

[239] Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P., *o.c.*, p. 49.

[240] Commission of the European Communities, 'Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market', Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, 28 November 2008, COM(2008) 798 final, p. 6, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF.

[241] Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P., *o.c.*, p. 51.

7.4 Internal market

7.4.1 Country of Origin

Article 4 (1) of the E-Signature Directive provides that 'each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive'. This provision introduces a 'country of origin' principle for the regulation of certification service providers similar to the one provided by the E-Commerce Directive in relation to information society services.[242] It entails that certification service providers are subject to the national legislation of the jurisdiction in which they are established and that other Member States may not prevent them from offering services within their jurisdictions through rules governing the provisioning of certification services which are harmonized by the E-Signature Directive.[243]

7.4.2 Free circulation of electronic signature products

Article 4, 2 stipulate that Member States must ensure that electronic signature products which comply with this Directive are permitted to circulate freely in the internal market.[244] Whereas article 4, 1 concerned the free movement of certification services, this provision concerns the free circulation of electronic signature products.

Art. 3, 5 provides that the Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognized standards for electronic-signature products in the Official Journal of the European Communities. When an electronic signature product meets those standards, Member States are obliged to presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III.[245]

The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States (article 3, 4). The E-Signature Directive mandates the Commission to, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated. It has since exercised this mandate by means of Decision 2000/709/EC.[246]

---

[242] Compare *supra*; section 6.3.

[243] Oversight and/or accreditation schemes in particular should not lead to legal or practical barriers for the provisioning of certification services within the internal market.

[244] The requirement of free circulation of electronic signature products is without prejudice to the regulations regarding dual-use goods as contained in Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods (5) and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods.

[245] The scope of art. 3, 5 is in principle limited to electronic signature products that have to meet the requirements specified in those annexes. However, the European Commission is in principle free to issue recommendations or deliver opinions on the application of standards beyond the scope of art. 3, 5. These recommendations or opinions will not have the same legal effect as those made pursuant to art. 3, 5 (presumption of compliance), but may fulfil a similar role in practice. (See Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P., *o.c.*, p. 45.)

[246] Commission Decision of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of

7.5 No prior authorization

Article 3 of the E-Signature Directive provides that Member States shall not make the provision of certification services subject to prior authorization. 'Prior authorization' is understood as any requirement mandating certification-service-providers to obtain a decision by national authorities before being allowed to provide certification services or any other measures having the same effect.[247] This provision reflects one of the basic tenets of the Directive, namely that the recognition of electronic signatures should be based upon objective (rather than administrative) criteria.[248]

7.6 Oversight

While the Directive prohibits the institution of prior authorization schemes, it does require Member States to introduce an appropriate system of supervision of CSPs which issue qualified certificates to the public (article 3, 3). In other words, Member States are expected to ensure that CSPs established within their territory abide by the requirements set forth by the Directive, but are prohibited by exercising supervision by means of a prior authorization scheme or other oversight mechanisms which have a similar effect.[249] Besides these restrictions, Member States are free to decide how supervision shall be organized.[250]

Article 3, 3 only requires oversight of CSPs offering qualified certificates to the public. While Member States in principle remain free to extend to oversight tasks of supervisory bodies to other types of services offered by CSPs, the Directive by no means requires them to do so.[251] This provision illustrates that the main concern of the drafters of the Directive was to ensure that the public can trust the validity of certificates which have been designated as being 'qualified'.

7.7 Voluntary accreditation

The Directive also does not prohibit Member States from introducing or maintaining voluntary accreditation schemes aiming at enhanced levels of certification-service provision (art. 3, 2). Article 3, 13 of the Directive defines 'voluntary accreditation' as 'any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where

---

the European Parliament and of the Council on a Community framework for electronic signatures, *O.J.* 16 November 2000, L 289/42-43.

247 Recital (10) of Directive 1999/93/EC. Compare also art. 4 of the E-Commerce Directive (cf. *supra*; section 6.4).

248 See also recital (21) of Directive 1999/93/EC.

249 Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P., *o.c.*, p. 38.

250 *Ibid*, 40. Recital (13) of Directive 1999/93/EC indicates that the Directive also does not preclude the establishment of private-sector-based supervision systems.

251 *Ibid*, 39.

the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body'.

The rationale behind art. 3, 2 is that voluntary accreditation schemes may offer CSPs the appropriate framework for further developing services towards the levels of trust, security and quality demanded by the evolving market. Such schemes should encourage the development of best practice among certification-service-providers.[252]

The recitals of the Directive further stipulate certification-service-providers should be left free to adhere to and benefit from such accreditation schemes.[253] As a result, Member States should not prohibit CSPs from operating outside voluntary accreditation schemes. In addition, it should be ensured that such accreditation schemes do not reduce competition for certification services.[254]

In any event, any conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited CSPs for reasons which fall within the scope of this Directive (art. 3, 2). For example, an accreditation scheme instituted in one Member State, which is restricted to CSPs established there, would arguably violate this provision.[255]

7.8 Liability of CSPs

Article 6 of the E-Signature Directive regulates several liability aspects related to the issuance of (and reliance upon) qualified certificates. On the one hand, this article establishes the minimum liability exposure for CSPs issuing qualified certificates to the public (or by guaranteeing such a certificate to the public) in its relation to relying parties. On the other hand, article 6 also establishes certain limitations on the liability of CPSs concerning the issuance of qualified certificates which Member States must recognize.[256]

7.8.1 Minimum liability exposure

Article 6, 1 requires Member States to ensure that a CSP issuing a certificate as a qualified certificate to the public (or by guaranteeing such a certificate to the public) shall be liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

a) as regards the *accuracy* at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
b) for assurance that at the time of the issuance of the certificate, the *signatory* identified in the qualified certificate *held the signature-creation data* corresponding to the signature-verification data given or identified in the certificate;
c) for assurance that the *signature-creation data and the signature-verification* data can be used in a *complementary* manner in cases where the certification-service-provider generates them both.

[252] Recital (11) of Directive 1999/93/EC.
[253] Id.
[254] Recital (12) of Directive 1999/93/EC.
[255] Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P., *o.c.*, p. 39.
[256] *Ibid*, 51. 5. The provisions of paragraphs 1 to 4 are without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *O.J.* 21 April 1993, L 95/29.

The above applies unless the certification-service-provider is able to prove he has not acted negligently.

Art, 6 2 provides that a CSP who has issued a certificate as a qualified certificate to the public shall at a minimum be liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for *failure to register revocation* of the certificate, unless the certification-service-provider proves that he has not acted negligently.

Reviewing these provisions, one can derive the following conditions for the minimum liability scheme of art. 6, 1 and 6,2 to be applied[257]:

- the certificate must have *been issued by the CSP as a qualified certificate*: whether a certificate is actually qualified or not is irrelevant, what is decisive is whether or not it was designated as a qualified certificate by the CSP;
- the certificate must be have been *issued or guaranteed to the public*[258]:
  a) a certificate may be considered to have been 'issued to the public' if its intended use is not limited to relying parties/verifiers with whom the CSP has an established contractual relationship;
  b) a certificate may be considered as being 'guaranteed to the public': the scope of this guarantee may be derived by consulting the CSP's Certificate Practice Statement (CPS);
- the plaintiff must show that harm resulted from one of the liability causes enumerated in article 6, 1 (i.e. accuracy and completeness of the information in the qualified certificate, identity of the signatory and control over signature-creation data, complementary nature of signature-creation and –verification data in cases where the CSP generates them both) or 6, 2 (i.e. failure to register revocation);
- the plaintiff must be able to show that her reliance upon the certificate in question was in fact 'reasonable'.

The CSP can escape liability under both article 6, 1 and 6, 2 if he can prove that he has not acted negligently. In other words, the Directive does not impose a strict liability upon the CSP, but does place the burden of proof upon the CSP to demonstrate it has exercised appropriate diligence.[259]

7.8.2 Limitations of liability

Article 6, 3 and 6, 4 of the E-Signature Directive explicitly recognize two ways in which a CSP issuing qualified certificates may limit his liability. These limitations have to be recognized in each of the Member States provided that they are included in the certificate itself in a form that is recognizable to third parties.[260]

The first way in which a CSP might limit his liability is by incorporating *limitations on use* in the certificate. Article 6, 3 provides that a CSP shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it (provided these limitations are indicated in the certificate and recognizable to third parties).

---

257 Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P., *o.c.*, 52-53.

258 Article 6, 2 does not make any reference to being 'guaranteed to the public'. Therefore the plaintiff will have to show that the CSP issued the qualified certificate to the public.

259 Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P., *o.c.*, 55.

260 *Ibid*, 55.

The second way in which a CSP might limit his liability is by incorporating *limitations on the value of transactions* for which the certificate can be used. According to article 6, 4, the CSP shall not be liable for damage resulting from this maximum limit being exceeded (provided these limitations are indicated in the certificate and recognizable to third parties).

7.9 Entity Authentication?

An interesting question to consider is the extent to which the E-Signature Directive might be held applicable to entity authentication mechanisms. On a conceptual level, a distinction is often made between data (origin) authentication and entity authentication. Data (origin) authentication has been described as a mechanism which provides assurance, through corroborative evidence, of the identity of the entity from which a message (data) originates.[261] Entity authentication on the other hand can be described as a process that corroborates the claimed (partial) identity of an entity.[262] In other words, the conceptual distinction between data and entity authentication refers to the goal of the authentication: corroboration of the origin of data vs. corroboration of the (partial) identity of an entity.

While this conceptual distinction may appear relatively clear, several clarifications are necessary to properly explain the relationship between the two types of authentication. The first is that both types of authentication can (but do not necessarily) rely on digital signature techniques.[263] In other words, certain digital signature techniques can be used both for purposes of data (origin) authentication and for purposes of entity authentication. For example, public-key infrastructures (PKIs) can in principle be used for both these purposes. In case of entity authentication, corroboration of the identity of entity is derived (inter alia[264]) from the fact that the entity is able to digitally sign (a hash value of) a challenge which establishes control over the relevant private key (i.e. the private key corresponding with the public key that has been associated the identity that is being claimed). In case of data (origin) authentication, the procedure is largely identical: given a unit of data signed using a private key, the recipient can verify its origin (authenticity and

---

[261] Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *o.c.*, p. 25. Data origin authentication implicitly also provides data integrity: if the message were to have been modified during transmission it could not be said to have originated from that same entity (*Ibid*, 25.)

[262] Modinis Study on Identity Management in eGovernment, 'Common Terminological Framework for Interoperable Electronic Identity Management', consultation paper prepared for the eGovernment Unit DG Information Society and Media of the European Commission, v2.01, 23 November 2005, p. 7, published online at: https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf.

[263] A digital signature is data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit. (X. Huysmans and B. Van Alsenoy (eds.), 'D1.3 Conceptual Framework – Annex I. Glossary of Terms', *l.c.*, p. 15. See also Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *o.c.*, p. 22-23.) The term 'signature' different meanings with different audiences. Regarding the different meanings associated to the term 'signature' by lawyers and computer scientists respectively see also Meints, M. and Hansen, M. (eds.), 'D3.6 Study on ID Documents', Future of Identity in the Information Society (FIDIS) deliverable, 2006, p. 72-73, available at www.fidis.net. For the purposes of this report, we shall use the term 'digital' signatures when referring the cryptographic technique, whereas the term 'electronic' signature shall be used to the legal concept of a signature as defined by Directive 1999/93/EC and/or national Member State legislation.

[264] The final level of entity authentication assurance is determined by a variety of factors, not just the type or strength of the authentication mechanism used. See e.g. W.E. Burr, D. F. Dodson and W.T. Polk, Electronic Authentication Guideline, NIST SP800-63, v1.0.2, available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

integrity) by applying the public key to the signed data (typically a hash value of the original message), and by corroborating that the signer's certificate has not been revoked.

The E-Signature Directive defines an electronic signature as 'data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication' (article 2, 1). An advanced electronic signature is defined as an electronic signature which (a) is uniquely linked to the signatory; (b) is capable of identifying the signatory; (c) is created using means that the signatory can maintain under his sole control; and (d) is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable (art. 2, 2). Given these definitions, it might be argued that the scope of the Directive encompasses both entity authentication and data origin authentication mechanisms in so far as they rely on electronic (digital) signature techniques.[265] However, there are a number of arguments which might be made against this proposition. The first is that recital (4) of the Directive situates the rationale for the Directive in the context of data authentication rather than entity authentication.[266] The second is that the Directive, despite the fact that several of its provisions have clearly been inspired by existing digital signature mechanisms, addresses the signature as a legal concept, rather than a technical one.[267] Finally, even if the proposition that the E-signature Directive seeks to regulate electronic (digital) signature mechanisms in general were to be accepted, its current relevance would be limited as the key provisions of this Directive mainly concern the role of these mechanisms for purposes of data origin authentication.[268]

In conclusion it should be noted that the Digital Agenda recently unveiled by the EU Commission proposes a revision of the Directive on E-Signatures. The goal of this revision would be 'to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems'.[269] The current problem of cross-border authentication in the context of online public services is expected to be addressed by 'a Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector)'.[270]

---

[265] See also T. Myhr, 'Regulating a European eID - A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID', Study for the Porvoo e-ID Group, 31 January 2005, p. 12-13, available at www.fineid.fi/default.aspx?id=0&docid=3847&action=Publish.

[266] See also Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P., *o.c.*, 29 and Commission of the European Communities, 'Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market', *l.c.*, p. 4 ('*To be a signature the authentication must relate to data and not be used as a method or technology only for entity authentication.*'). The validity of this argumentation can in principle be questioned in light of the finding that certain entity authentication protocols rely, to a large extent, on data (origin) authentication mechanisms. However, on may nevertheless argue that, by explicitly referring to data authentication, the rationale of the EU legislator was to refer to use of mechanisms which establish appropriation by the signatory rather than use of the same mechanisms for the purposes of providing/obtained corroboration of a claimed (partial) identity.

[267] Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P., *o.c.*, 29. See also H. Graux, J. Majava, E. Meyvis (eds.), 'Study on eID Interoperability for PEGS: Update of Country Profiles - Analysis & assessment report', *l.c.*, 107-108.

[268] Meints, M. and Hansen, M. (eds.), 'D3.6 Study on ID Documents', *l.c.*, p. 74. See also H. Graux, J. Majava, E. Meyvis (eds.), 'Study on eID Interoperability for PEGS: Update of Country Profiles - Analysis & assessment report', *l.c.*, 108.

[269] European Commission, 'A Digital Agenda for Europe', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 19 May 2010, COM(2010) 245, p. 11, available at http://ec.europa.eu/information_society/digital-agenda/index_en.htm.

[270] *Ibid*, 32.

7.10 Relationship Directive 95/46/EC

Article 8, 1 of the E-Signature Directive provides that Member States shall ensure that CSPs and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC. In addition to this general statement of applicability of the Data Protection Directive, the E-Signature Directive also includes a number of specific provisions containing data protection requirements for the practices of CSPs.

Article 8, 2 specifies that Member States must ensure that a CSP which issues certificates to the public 'may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject'. In other words, the E-Signature Directive limits the basis of legitimacy of processing by the CSP to data subject consent. It also mandates direct collection of information from the data subject, unless she has explicitly authorized indirect collection.

Annex II of the E-Signature Directive further specifies that the CSP issuing qualified certificates must use trustworthy systems to store certificates in a verifiable form so that:

- only authorized persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

Finally, article 8, 3 of the E-Signature Directive that Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name. This prohibition is however without prejudice to the legal effect given to pseudonyms under national law, as well as requirements under Community or national law requiring identification of persons.[271]

7.11 Implications

At the beginning of this chapter we indicated that the extent to which Directive 1999/99/EC is directly relevant to the deployment of INDI Services may be limited. The deployment of INDI Services may of course indirectly benefit from this Directive's provisions, in that it further promotes the recognition of electronic contracts. However, the majority of the services envisioned by GINI do appear to fall outside the scope of this Directive.

The situation shall be slightly different to the extent that one of the actors involved in the PIM ecosystem is qualified as a certification service provider (CSP) within the meaning of the E-Signature Directive. This term is defined very broadly by the Directive, as 'an entity or a legal or natural person who issues certificates *or provides other services related to electronic signatures*' (art. 2, 11). The term 'electronic signatures' is also defined very broadly by the Directive (cf. *supra*), on the

[271] See also recital (25) of Directive 1999/99/EC.

basis of which one might argue that "the potential of a certain method to serve authentication purposes is the only functional condition imposed by the directive's definition for this method to be qualified as 'electronic signature', irrespective of its intrinsic capabilities to generate or not the legal effects of a signature".[272] Under such a broad interpretation one might argue that both INDI Operators and Data Sources can qualify as certification service providers within the meaning of the Directive. After all, it may be expected that several of the services of these actors have 'the potential to serve authentication purposes', as they aim to enable INDI Users to present corroborative evidence to relying parties concerning their identity and/or other attributes.

However, we have also discussed a number of arguments against such a broad interpretation. The main argument is that Directive 1999/93/EC seeks to addresses the signature as a legal concept, rather than a technical one.[273] Although a literal reading of the Directive's definitions of 'electronic signatures' and 'certification service providers' supports a broad applicability of the Directive, a teleological interpretation mandates that its scope be limited to signature mechanisms services which seek to generate, maintain, or otherwise support the equivalent legal effect a handwritten signature.

In any event, even if it were accepted that either the INDI Operator or the Data Source acts as a certification service provider, the practical relevancy of this conclusion would still be limited. Article 5 of the Directive is clearly limited to the legal effects of electronic signatures as a legal concept. The scope of article 6 is limited to CSPs issuing qualified certificates. Article 8 applies to all CSPs issuing certificates to the public, but mainly imposes the additional requirement of reliance upon consent – a requirement which shall already met by the design choice that consent shall serve as a default basis for the processing in the context of INDI services.[274] The remaining substantive provisions of Directive 1999/93/EC concern the internal market and the prohibition of prior authorization, for which there exist provisions with a similar effect under Directive 2000/31/EC.[275]

7.12 Legal barriers and gaps

Under this section we wish to evaluate the extent to which the 'certification' services offered by an INDI Operator or Data Source require additional regulation. At the beginning of this section, we indicated that there is a conceptual similarity among the certification services envisioned by Directive 1999/93/EC and those provided by the INDI Operator and the Data Source respectively. The term 'digital certificate' is most often used in reference to public-key digital certificates. On a conceptual level however, the role of a certificate is to attest to the truth of certain stated facts. Therefore the attestations contained in 'certificates' (in the broad sense) can in principle relate to any characteristic or event one wishes to see certified.

The PIM ecosystem envisioned by GINI aims to enable users to present corroborative evidence regarding their identity or attributes towards relying parties, by enabling them to present links to information maintained by either private- or public sector bodies. The aim of such a service is to increase the level of confidence for the relying party as to the identity and/or attribute of the

[272] See T. Myhr, *l.c.*, p. 12 (referencing Draft document CEN/ISSS WS/E-Sign WSES N 0383 (Turin 2003-12-16); Title CEN/ISSS WS/E-Sign Area AB "Evidential Value of Electronic Signatures" Version 0.07 November 2003, at p. 12).
[273] Cf. *supra*; section 7.9.
[274] Cf. *supra*; section 4.4.1.
[275] Cf. *supra*; sections 6.3-6.4.

individual in question. The INDI Operator shall contribute to this functionality by enabling the user to present such links, and verifying that the data is in fact maintained by the Data Source in question, or at least authenticate the source itself. The Data Source, from its part, will confirm or deny whether or not the asserted identity or attribute is true. In both cases, one could qualify this scheme as a third-party certification model: the relying party will rely on the INDI Operator and/or Data Source respectively to obtain assurance regarding the accuracy of a claim asserted by or about the user. This finding gives rises to the question of whether, and if so how, the 'certification' services offered by these actors should be made subject to additional regulation.

When considering the need for additional regulation for this type of certification services, it is useful to examine the reasons why the EU legislator felt it necessary to regulate certain certification services in relation to electronic signatures. One of the objectives of the drafters of the E-Signature Directive was to promote the use electronic signatures within the internal market, by creating a legal framework which contributes to the general acceptance and confidence in electronic signature technologies. As argued in the preceding sections, the term 'signature' in this Directive is aimed at addressing the legal concept of signatures, rather than the technical one (despite the fact that the similarity between several provisions of the Directive and certain digital signature mechanisms which have general purpose applications can hardly be overlooked). The need for recognition and regulation of electronic signature techniques stems from the fact that (legal) signatures fulfil a fundamental role in the legal order of most Member States. The EU legislator has by no means strived for complete harmonization in this area, but has sought to establish a number of parameters to promote their recognition and acceptance. In only one instance has the EU legislator in fact mandated a finding of equivalency vis-à-vis handwritten signatures, namely in the case of qualified signatures. The 'certification services' that would be performed by the INDI Operator and/or Data Source shall in principle be of an entirely different nature than the certification offered by CSPs issuing certificates for electronic signature purposes. The former are not aimed at facilitating the use of legally valid signatures, but rather to support the reliance upon an asserted identity or attribute, which is an entirely different functionality altogether.

The perceived need for regulation of electronic signatures was predicated to a large extent on the finding that electronic signatures require recognition beyond 'closed systems', where parties have the ability to negotiate the legal effects that should be associated with the use of a particular technology or processing operation. Recital (16) of the E-Signature Directive provides as follows:

> '*This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised; play an important role*' [emphasis added]

The trust model in the PIM Ecosystem envisioned by GINI is an operator-based trust model (i.e. a 'brokered' trust relationship).[276] The implementation model currently envisioned by the project specifies that in order to connect to the INDI infrastructure/network, an entity must have a contractual relationship with at least one INDI Operator. This contractual relationship should be sufficient for reaching the whole INDI space. In other words, the PIM Ecosystem envisioned by GINI is a 'closed system', which allows the relevant parties to specify the terms and conditions

[276] Cf. *supra*; section 2.2.

under which the services shall be offered. These terms and conditions shall in principle be recognized as long as they respect the boundaries set by the mandatory provisions of the applicable national law. On this basis, the need for additional regulation in support of the 'certification services' offered by INDI Operators and Data Sources would primarily arise to the extent there is:

- a specific need to derogate from the contractual freedom of parties in order to attain a legitimate policy objective, or
- a rationale arises for policymakers to increase the trustworthiness of services envisioned by GINI in order to stimulate their acceptance in an 'open' environment. For instance, in this scenario, additional regulation might be needed if the interests of relying parties were to be insufficiently protected under existing legislation.

8 Conclusion

The objective of this deliverable has been to analyse the main legal requirements affecting the development of a PIM ecosystem and the provisioning of INDI Services. To this end, four areas of EU regulation have been investigated, namely:

- Data protection and privacy;
- Re-use of public sector information;
- e-Commerce; and
- Electronic signatures.

The purpose of our analysis was not only to identify relevant legal requirements, but also to articulate potential barriers and gaps. Over the following paragraphs, we will reiterate our main findings from this perspective for each of the identified areas of regulation.

The strongest regulatory impact on the provisioning of INDI Services will result from data protection and privacy requirements. For the most part, these requirements do not present actual barriers to the development INDI Services. They mainly entail the need for a clear allocation of roles and responsibilities to ensure that the obligations of each entity under data protection and privacy law are met. Practical barriers are likely to arise due to lack of harmonization in implementation (e.g., divergent consent requirements) or legal uncertainty (e.g., determination of the legal qualification of each actor). However, the legal barriers in this area result more from sector-specific requirements rather than general data protection or privacy requirements. The most prominent examples in this regard are the regulation of use of personal data by public sector bodies and the use of identifiers of general application.

The European regulatory framework on the re-use of public sector information will also impact the development of INDI Services insofar as they seek to make use of identity or other personal data maintained by public sector bodies. This framework aims to ensure a level playing field for actors seeking to re-use PSI for commercial (or non-commercial) purposes. These provisions may in principle benefit INDI Operators as well as the other actors that play a role in the PIM ecosystem. However, it is clear that a number of legal barriers and gaps remain. These barriers and gaps all revolve around the same issue, namely the absence of a regulatory framework which enables and promotes the re-use of PSI pursuant to a data subject request. In addition to the lack of an obligation to make available PSI, a number of legal barriers result from the restrictions contained in Directive 95/46/EC and art. 8 of European Convention of Human Rights. While taking note of these restrictions as potential obstacles, it is also important to consider that they were adopted to protect specific interests, often those of the data subjects themselves. When assessing these obstacles from a policy perspective, appropriate consideration must be given to these interests, as well as the need for adequate safeguards going forward. These issues will be revisited in the context of our next deliverable (D3.2).

The provisioning of INDI services shall also fall within the remit of the E-Commerce Directive. This implies that service providers such as INDI Operators shall in principle benefit from the internal market provisions established by the Directive; the general prohibition of a prior authorization scheme; as well as the provisions on electronic contracting. It also implies that these actors will have to comply with the substantive requirements set forth by this Directive, such as the transparency obligations. Whether or not any of actors involved in the PIM

ecosystem envisioned by GINI shall be able to avail themselves of the liability exemptions established by this Directive will depend on the actual implementation of INDI Services.

A final area of EU regulation investigated in this deliverable is the community framework on electronic signatures. We concluded that this framework, in its current form, has only little direct relevance to the deployment of INDI Services. However, we have also observed a conceptual similarity among several of the services offered by the actors of the PIM Ecosystem and those offered by 'certification service providers' as defined by Directive 1999/99/EC. When considering the need for additional regulation for this type of certification services, it is useful to take into account the reasons why the EU legislator felt it necessary to regulate certain certification services in relation to electronic signatures. We concluded that the need for additional regulation of the 'certification services' offered by INDI Operators and Data Sources should arise primarily to the extent there is:

- a specific need to derogate from the contractual freedom of parties in order to attain a legitimate policy objective, or
- a rationale for policymakers to increase the trustworthiness of services envisioned by GINI in order to stimulate their acceptance in an 'open' environment.